42 Yıllık Arşiv DVD'niz Derginizle Birlikte...



Bilim ve Teknik



500. SAYI

Aylık Popüler Bilim Dergisi
Temmuz 2009 Yıl 42 Sayı **500**
3,5 TL

Bilgi Güvenliği İçin Matematiksel Yaklaşım

Kriptoloji

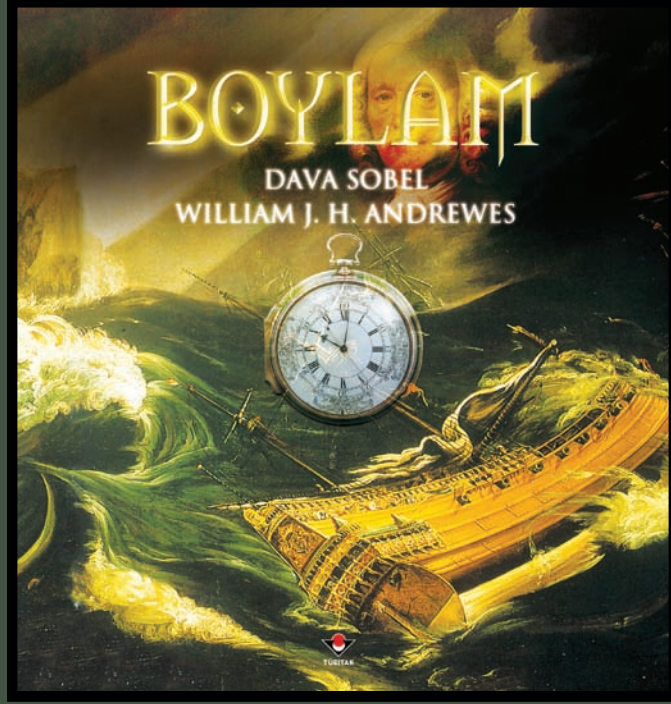


Kuantum Kriptoloji

Teletıp

Hayvancılıkta Gen Çağı


ISSN 13003380



Boylam *on yedinci ve on sekizinci yüzyılın*
en zorlu bilimsel problemini çözme yolundaki çabaları anlatıyor.

Büyük keşif çağı boyunca denizciler okyanuslarda
bulundukları boylamı hesaplayabilecekleri herhangi bir araç olmadan dolaştılar.
Pek çok bilim adamı boylam sorununun gökyüzündeki yıldızların
düzenli olarak gözlenmesiyle çözüleceğini düşünür ve bu yolda araştırmalar yaparken,
John Harrison adında bir adam inanılmazı yaptı:
Bugün kronometre dediğimiz,
denizde zamanı kesin olarak bilmeye yarayan bir saat.
İşte bu kitabın konusu
Harrison'ın bu yoldaki kırk yıl süren çabası.

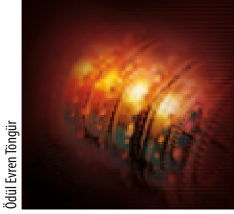


TÜBİTAK
POPÜLER BİLİM KİTAPLARI

Bilim ve Teknik

Aylık Popüler Bilim Dergisi
Yıl 42 Sayı 500
Temmuz 2009

"Benim mânevi mirasım ilim ve akıldır" *Mustafa Kemal Atatürk*


Ödül Evren Töngür

Değerli Okurlarımız,

Bilim ve Teknik dergisi 500. sayıya ulaştı. TÜBİTAK'ın kuruluş kanunundaki "Yurdumuzda yetişen gençlerin, kabiliyetlerini ve eğilimlerini bilimsel ve teknik araştırma alanlarına yöneltmek, bu konularda çalışma hevesini gençlik arasında yaymak ve en genel anlamda bilimsel ve teknik çalışmaları halka tanıtmak ve buluşlara yeniliklere ilgi duyan aydın kişilere aradıkları bilgiyi popüler bir dille ve doğru olarak verebilmek amacıyla yayınlar yapmak" maddesinden hareketle 1967 yılının Ekim ayında ilk sayısı yayımlanan dergimiz görevinin bilinciyle 42 yıldır her ay sizlerin karşısına çıkıyor.

Dergimize yayımlanması amacı ile gönderilen yazılarla birlikte *Bilim ve Teknik* dergisi yazarlarının hazırladıkları yazıların Yayın Kurulu'nun görüşüne sunulması ve o sayıda yayımlanacak yazıların belirlenmesi ile başlayan süreç, yazıların popüler hale getirilmesi ve redaksiyonunun yapılması ile devam eder. Düzeltilmiş yazıların grafiker tarafından sayfa düzeni hazırlanır ve sayının içeriğine uygun kapak tasarımı yapılır. Hazırlıkları tamamlanan dergi Yayın Kurulu üyelerinin görüşüne sunulur. Yayın Kurulu'nun onay vermesi üzerine derginin basım ve dağıtımı yapılır.

Bilim ve Teknik dergisi ekibi olarak sizlere dergimizin 500. sayısını sunmanın mutluluğunu ve heyecanını yaşıyoruz. Bizlere bu mutluluğu ve heyecanı yaşatan okurlarımıza 500. sayımızla birlikte dergimizin 42 yıl içinde yayımlanan 2008 yılının son sayısına kadar olan 493 sayıyı kapsayan arşiv DVD'sini hediye etmek bize ayrıca mutluluk veriyor. İlk sayısından son sayısına kadar derginin yayımlanmasına katkıda bulunan TÜBİTAK yöneticilerine, Yayın Kurulu üyelerine, yayımlanmak üzere yazılarını gönderen değerli yazarlarımıza, dergi çalışanlarına ve emeği geçen herkese sonsuz teşekkürler.

Temmuz sayımızda ana tema olarak günlük hayatımızın hemen her alanında yararlandığımız "bilgi güvenliği" konusunu ele aldık. Bilgi güvenliğinin sağlanması binlerce yıldır zihinleri kurcalayan bir konu, teknolojinin gelişimi ile birlikte de günümüzde oldukça ilerlemiş durumda. Bu alandaki baş döndürücü ilerleme hiç şüphe yok ki gizli bilgilere erişim için şifre kırma konusunda da sürmekte. Bu sayımızda bilgi güvenliği üzerinde çalışan bir bilim dalı olan kriptolojinin tarihçesi, gündelik hayatta kullanımı, kriptonun olmazsa olmazı anahtarlama, kuantum bilgisayarları ve kuantum kriptoloji konularını anlatan yazılarımız yer alıyor.

Bilim ve Teknik dergisi ekibi adına siz sevgili okurlarımıza sevgi ve saygılarımı sunuyor, gıda konusunun yer alacağı 501. sayımızda buluşmak ümidiyle esenlikler diliyorum.

Adnan Bahadır

Yazışma Adresi
Bilim ve Teknik Dergisi
Atatürk Bulvarı
No: 221 Kavaklıdere 06100
Çankaya - Ankara

Tel
(312) 427 06 25
(312) 427 23 92

Faks
(312) 427 66 77

Satış-Dağıtım
(312) 467 32 46
(312) 468 53 00/1061-3438
Faks: (312) 427 13 36
TÜBİTAK Santral
(312) 468 53 00

Internet
www.biltek.tubitak.gov.tr
e-posta
bteknik@tubitak.gov.tr

ISSN 977-1300-3380

Fiyatı 3,50 TL
Yurtdışı Fiyatı 5 Euro.

Dağıtım: DPP A.Ş.

Baskı: İmpress Baskı Tesisleri
İmaj İç ve Dış Tic. A.Ş.
İmajas.com.tr
Baskı Tarihi: 25.06.2009

Bilim ve Teknik Dergisi, Milli Eğitim Bakanlığı [Tebliğler Dergisi, 30.11.1970, sayfa 407B, karar no: 10247] tarafından lise ve dengi okullara; Genelkurmay Başkanlığı [7 Şubat 1979, HRK: 4013-22-79 Eğt. Krs. Ş. sayı Nşr.83] tarafından Silahlı Kuvvetler personeline tavsiye edilmiştir.

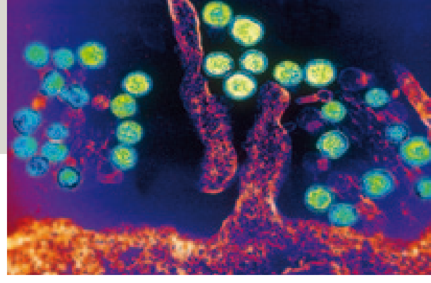
İçindekiler













Uzaylı Gözünden Dünya

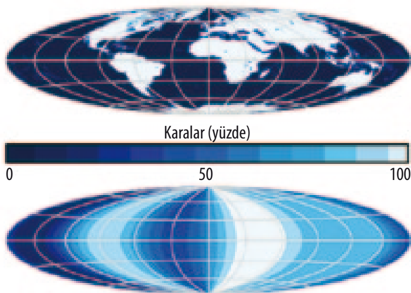
Alp Akoğlu

Su, yaşamın temel kaynağı. En azından bizim gezegenimizde böyle. Başka dünyalardaki yaşamın peşindeki araştırmacılar, bu gezegenlerde su olup olmadığını saptamanın yollarını arıyorlar. Bunun için çok uzaktaki bir gezegendeki olası okyanusların nasıl görüneceğini tahmin etmeye çalışıyorlar. Suya sahip bildiğimiz tek gezegen şimdilik Dünya olduğu için, onun uzaktan nasıl göründüğü araştırmacılara esin kaynağı oluyor.

Hartley 2 Kuyrukluyıldızı'nı incelemek üzere fırlatılan ve önümüzdeki yıl kuyrukluyıldıza ulaşması beklenen Deep Impact/EPOXI uzay aracı, yolculuğu sırasında boş durmayarak araştırmacılara bu konuda veri sağlıyor. Araç, kameralarını Dünya'ya çevirmiş durumda ve yaklaşık 50 milyon km uzaktan, gezegenimizin yüzeyinden yansıyan ışığın onun dönüşüne bağlı olarak nasıl değiştiğini izliyor.

Eğer bu araştırma başarılı olursa, giderek hız kazanan dünya benzeri ötegezegen araştırmalarına ışık tutacak. Yıldızının önünden geçen dünya benzeri ötegezegenleri saptayabilecek duyarlılıktaki Kepler Teleskobu, geçtiğimiz Nisan'da fırlatılmıştı. Kepler'le yapılan gözlemler sonucunda, birkaç yıl içinde Dünya benzeri ötegezegenlerin keşfedilmesi bekleniyor. Olası Dünya benzeri gezegenler keşfedilmeye başlandığında, bu araştırmalar daha da önem kazanacak.

Günümüzün teknolojisiyle, bir ötegezegenin yüzeyindeki herhangi bir ayrıntıyı doğrudan görüntüleyebilmemiz olanaklı değil. Ancak gezegenin yüzeyinin ışığındaki değişim, yüzeyinde en azından ekvator çevresinde bulunan okyanusların ve karaların birbirine oranı ve dağılımı gibi bilgileri sağlayabilecek. İşte bu nedenle kendi gezegenimize uzaktan bakma fırsatı bulmamız bu deneyimi kazanma açısından önemli.



http://www.scientificamerican.com/blog/60-second-science/post.cfm?id=spacecraft-turns-to-earth-to-see-wh-2009-06-01

Eski Yöntemle Yeni Gezegen

Alp Akoğlu

Ötegezegenleri arama yöntemlerinden biri olarak kabul edilen ve 50 yıldır denenen astrometri, nihayet ilk meyvesini verdi. Gökbilimciler bu yöntemi kullanarak Jüpiter benzeri bir ötegezegen keşfettiler.

Birbiri çevresinde dolanan iki gökcismi söz konusu olduğunda, genellikle küçük olanın büyük olanın çevresinde dolandığı söylenir. Eğer bu cisimler arasındaki kütle farkı büyükse, büyük kütleli cisim belirgin bir salınım yapmadığından bu ifade doğru kabul edilebilir. Gerçekte, birbiri çevresinde dolanan cisimler bir "ortak kütle merkezi" etrafında dolanırlar. Bu merkez, kütlesi büyük olan cisme daha yakındır.

İşte astrometri yöntemi, cisimlerin bu kütle merkezi çevresinde dolanırken yaptıkları salınımı ölçmeye dayanır. Birkaç ışık yılı uzaklıktaki bir gezegeni doğrudan gözlememiz şimdilik olanaklı olmadığı için, bir yıldızın gökyüzündeki çok küçük salınımları ölçülerek gezegenleri olup olmadığı ve varsa bu gezegenlerin kütleleri saptanabilir. Yöntem kuramsal olarak çok akla yakın olsa da, çok hassas ölçümler ve uzun süreli gözlemler gerektirdiğinden, çok denendiyse de ötegezegen araştırmalarında şimdiye kadar sonuç vermemişti.

San Diego yakınlarındaki Palomar Gözlemevi'ndeki teleskobu 12 yıldır astrometri çalışmaları için kullanan gökbilimciler, bu yöntemin işe yarayabileceğini gösterdiler. Otuz yıldızı dikkatle ve uzun süren gözlemlerle izleyen gökbilimciler bu yıldızlardan birinin çevresinde dolanan bir ötegezegen buldular.



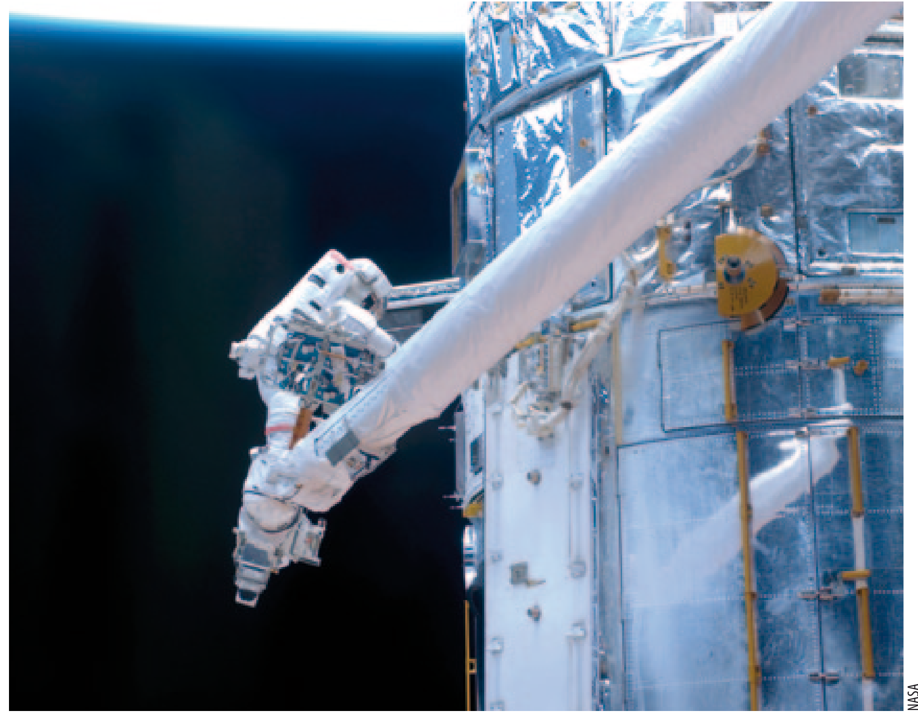
VB 10b adı verilen bu ötegezegen, Kartal Takımyıldızı'nda bulunuyor ve bize yaklaşık 20 ışık yılı uzaklıkta. Gezegenin kütlesi Jüpiter'inkinin yaklaşık altı katı ve yıldızına uzaklığı Güneş-Jüpiter uzaklığı kadar. Buna karşılık, sistemin yıldızı VB 10 bilinen en küçük kütleli yıldız; kütlesi Güneş'inkinin yalnızca 12'de biri kadar. VB 10, bir gaz kütlesinin yıldız olarak parlayabilmesi için kütle bakımından alt sınırda. Gökcisminin kütlesi daha küçük olsaydı, merkezindeki sıcaklık ve basınç çekirdek tepkimelerini başlatamayacak ve bir yıldız olamayacaktı. VB 10 böylece, gezegeni olduğu bilinen en küçük kütleli yıldız olma unvanını da kazanmış oldu.

Yıldızın küçük, gezegenin büyük olması yıldızın yaptığı salınımın büyük olmasını, dolayısıyla da ölçülebilir olmasını sağlıyor. VB 10, bu özellikleriyle astrometri için ideal bir örnek. Buna karşın, bu yıldızın yer değiştirmesini ölçmek bile bir insan saçının kalınlığını 3 km uzaktan ölçmeye benziyor. Bu yöntemle daha büyük kütleli yıldızların çevresinde dolanan daha küçük gezegenlerin keşfedilebilmesi için aygıtların duyarlılığının artması gerekiyor. Buna karşın araştırmacılar bu yöntemden umutlu. En azından şimdilik Jüpiter benzeri gezegenlerin bu yöntemle keşfedilebileceği kanıtlanmış oldu.

http://www.astronomy.com/asy/default.aspx?c=a&id=8316



NASA



NASA

Hubble Eskisinden Daha da İyi

Alp Akoğlu

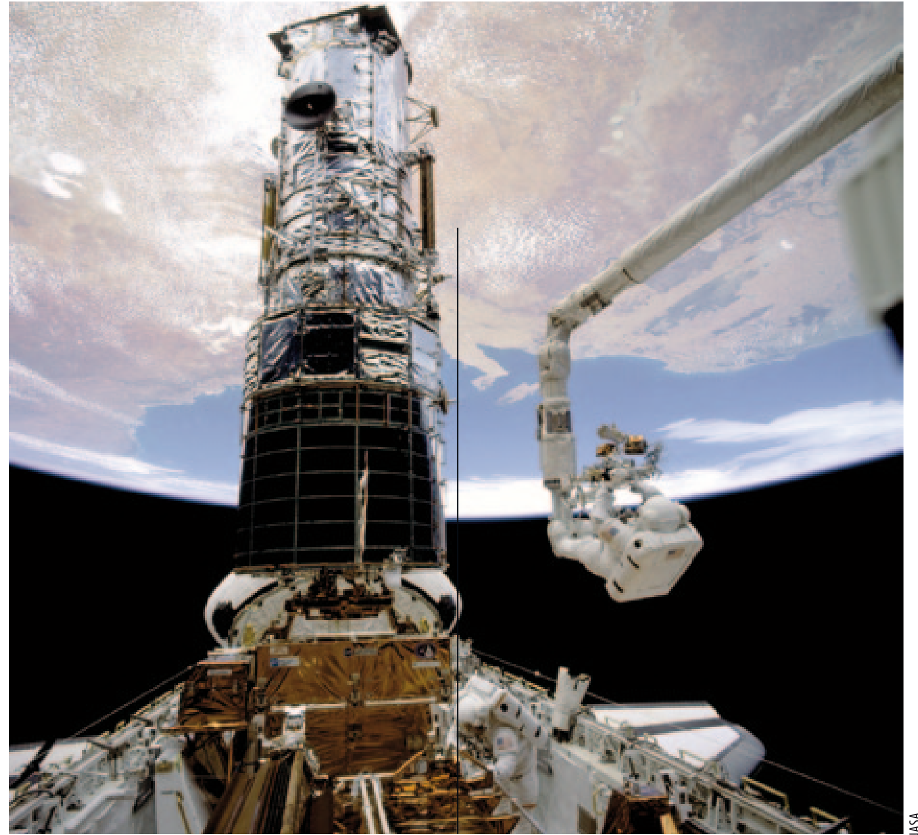
1990 yılında fırlatılan ve gökbilim araştırmalarında bir çığır açan Hubble Uzay Teleskobu, Mayıs ayında dördüncü kez bakımdan geçti. 11 Mayıs'ta fırlatılan Atlantis Uzay Mekiği'yle giden ekip, 13 gün uzayda kaldı ve bu süre içinde toplam beş kez uzay yürüyüşü yaparak teleskoba iki yeni aygıt ekledi. Astronotlar ayrıca, bozulan iki aygıtın tamirini yaptı ve eskiyen birçok parçayı değiştirdi.

Hubble'a eklenen iki aygıttan biri olan Geniş Alan Kamerası 3 (Wide Field Camera 3 - WFC3), aynı anda olmasa da hem kızılötesi, hem görünür, hem de morötesi ışınımı görüntüleyebilen yetenekli bir algılayıcı. Bu kamera, özellikle karanlık enerji ve karanlık madde araştırmalarında, yıldız oluşumunun anlaşılmasında ve çok uzak gökadaların keşfinde kullanılacak.

Eklenen öteki aygıt "Kozmik Kökenler Tayfçekeri" (Cosmic Origins Spectrograph - COS) olarak adlandırılıyor ve bu aygıtın kullanılmasıyla yapılacak gözlemlerin gökada evrimi, gezegen oluşumu, yaşamı oluşturan elementlerin ortaya çıkışı, gökadalar arası kozmik gaz ve birçok başka alanda yapılan araştırmalara önemli katkılar sağlaması bekleniyor.

Hubble'ın yenilenmiş haliyle yapılacak gözlemlerin Eylül'de başlaması bekleniyor. Eylül'e kadar, takılan yeni aygıtların ayarlamaları ve denemeleri yapılacak. Araştırmacılar, Hubble'ın bu haliyle eskisinden çok daha iyi olduğunu ve bir aksilik olmazsa 2014'e kadar başka bir bakıma gerek olmayacağını düşünüyorlar.

http://hubblesite.org/servicing_mission_4/



NASA


NASA

Güneş'ten Neden Uzaklaşıyoruz?

Pınar Dündar

Güneş ve Dünya arasındaki uzaklık gökyüzü gözlemcilerinin binlerce yıldır üzerinde düşündüğü bir konu. MÖ 3. yüzyılda güneş merkezli evren modelini ilk ortaya atan Samos'lu Aristarchus (M.Ö. 312-230), Ay'ın uzaklığıyla karşılaştırıldığında Güneş'in Dünya'dan 20 kez daha uzak olduğu tahmininde bulunmuştu.

20. yüzyılın sonlarında gökbilimciler, "astronomi birimi" olarak da adlandırılan bu kozmik uzaklıkla ilgili çok daha iyi bir noktaya geldiler.

Günümüzde, Güneş Sistemi'ni oluşturan tüm gökcisimlerinin uzaklıkları radarlar ve uzay araçları sayesinde dikkate değer bir duyarlılıkla bilindiği gibi, Güneş-Dünya uzaklığı da çok küçük bir hata payıyla belirlendi. Şu anki değer yaklaşık 149.597.870,696 km; hata payıysa sadece 0,1 metre.

İşte bu kadar hassas ölçüm yapılabilmesi sayesinde, 2004 yılında Güneş ve Dünya'nın birbirinden giderek uzaklaştığı saptandı. Her ne kadar küçük bir miktar, yılda sadece 15 cm, olsa da ölçüm hatasından 100 kez daha büyük olduğundan, bir şey Dünya'yı gerçekten de dışarı doğru itiyor olmalı. Ama ne?

Bu konudaki bir görüşe göre Güneş, parlamalarla uzaya yaydığı parçacıklar nedeniyle kütleçekim gücünü kaybediyor. Öte yandan yerçekimi sabiti G'nin değişmesi, evrenin genişlemesi ve hatta karanlık maddenin etkisi öne sürülen farklı açıklamalardan bazıları.

Ancak Takaho Miura ve ekibi cevabı bulduklarını öne sürüyor. Astronomy & Astrophysics adlı dergide yayımlanan makalelerinde Güneş ve Dünya'nın gelgit etkileşimi sonucu birbirlerini ittiklerini belirtiyorlar. Açıklamalarına göre buna yol açan mekanizma, Ay'ın yörüngesini dışarıya doğru iten süreçle aynı: Ay'ın çekimi sonucu okyanuslarda oluşan gelgitler Dünya'nın dönüş enerjisini giderek Ay'ın hareketine aktarıyor. Sonuç olarak Ay'ın yörüngesi yılda yaklaşık 4 cm genişlerken Dünya'nın dönüşü 0,000017 saniye yavaşlıyor.

Benzer şekilde, Miura'nın ekibi, gezegenimizin kütlesinin Güneş üzerinde küçük ancak sürekli bir gelgit kabarması oluşturduğunu varsayıyor. Hesaplamalarına göre, Güneş'in dönüş hızı Dünya sayesinde yüzyılda 3 milisaniye yavaşlıyor.

http://www.skyandtelescope.com/news/46618862.html

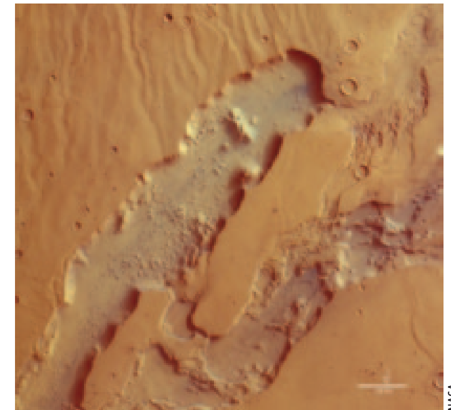
Mars'ta Antifriz

Özden Hanoğlu

Gezegenbilimcilerin büyük bir çoğunluğu Mars'ın Güneş Sistemi'nde yaşam bulundurma olasılığı en yüksek yer olduğu görüşündeler. Ama bir sorun var; Kızıl Gezegen hiçbir zaman Dünyamızın barındırdığı canlı türlerini barındıracak kadar ısınamamış olabilir. Yine de bu Mars'ta akan sular yoktu anlamına gelmiyor. Yeni bir araştırmaya göre Mars'ın suları çok fazla tuz içeriyordu ve bu tuz antifriz görevi görmüş olabilir.

Mars kayalarının ve maden yataklarının incelenmesiyle doğan antifriz fikrini ortaya atan bilim insanları, NASA ve iki İspanyol enstitüsünün çalışanları. Araştırmacılar, gezegenin dört farklı yerinde yürütülen Spirit, Opportunity, Viking 1 ve Pathfinder görevlerinde toplanan verileri bir araya getirdiklerinde bunların oldukça tutarlı olduğunu görmüşler. Dört yerin her birinde de aynı dokuz elementin (silikon, demir, kükürt, magnezyum, kalsiyum, klor, sodyum, potasyum ve alüminyum) yüzey kayaçlarının yapısının çoğunluğunu oluşturduğunu belirlemişler. Araştırmacılar, bu elementlerin kimyasal etkileşimlerinin sıfırın çok altındaki derecelerde bile suyu donmaktan koruyabileceğini aktarıyorlar.

Araştırmacılar, gezegenin sıcaklık ölçümü verilerinden yararlanarak bilgisayar yardımıyla iklimleme modellemeleri de oluşturmuşlar. Modellemeler, gezegenin atmosferinin hep ince olduğunu ve donma sıcaklığı üzerindeki sıcaklıkları destekleyemeyeceğini gösterse de uydu fotoğraflarında yer alan nehir yataklarını ve deltaları andıran yer şekilleri, gezegen yüzeyinde bir zamanlar suyun


NASA

aktığına dair güçlü iddialar sunuyor. Araştırmacılar, modellemeler ve yüzeyde akan su fikrini bağdaştırabilmek için Mars yüzeyindeki suyun çok tuzlu olduğunu ve donmadığını öngörüyorlar. Zamanla gezegenin sıcaklığının bugünkü seviyesine indiği (ortalama -60°C; gündüz ekvator bölgesindeki sıcaklık 20°C'ye kadar çıkabiliyor; kutuplardaysa -125 °C'ye kadar düşebiliyor) sonunda suyun donduğu ve buharlaşarak geriye söz konusu maden yataklarını bıraktığı görüşündeler.

Bilim insanları arasında bu görüşe sıcak bakanlar var, ancak günün birinde bu maden yataklarının oluşumuna başka açıklamalar getirilebileceğini de ekliyorlar.

http://sciencenow.sciencemag.org/cgi/content/full/2009/520/3?rss=1
http://www.nasa.gov/topics/moonmars/features/mars_freeze_052709.html
http://www.nasa.gov/worldbook/mars_worldbook.html


Jupiterimages

Atmosfer İncelirse Biyosfer Kurtulur mu?

İlay Çelik

Bundan 100 milyon yıl ila 1 milyar yıl sonra, Dünya'nın atmosferinden o kadar fazla karbondioksit eksilmiş olacak ki bitkiler ve ağaçlar sözcüğün tam anlamıyla boğulmaya başlayacak ve sonunda Dünya'daki yaşam da onlarla birlikte bitecek. Yapılan yeni bir araştırmada bu sonu geciktirmek için bir yol öneriliyor: Atmosfer basıncını azaltmak.

Dünya'nın jeolojik tarihi boyunca atmosferdeki CO_2 seviyesi düşüş gösterdi. Bugünkü konsantrasyonlar milyarlarca yıl öncekinin çok küçük bir yüzdesi kadar. Bitkiler, algler ve fotosentez yapan diğer canlılar CO_2 tüketir ancak bu canlılar ölünce CO_2'in büyük kısmı sonuçta tekrar atmosfere döner. O halde CO_2'i kalıcı olarak tutan başka bir süreç var. Eldeki kimyasal bulgular kayaçlardaki silikayı işaret ediyor: Bileşikler karbonu bir şekilde bikarbonata çeviriyor ve böylece biyosferden uzaklaştırıyor. Araştırmacılar bu eğilim devam ederse Dünya'da bir milyar yıl sonra fotosentez yapılamayacağını gösterdi.

Pasadena'daki Kaliforniya Teknoloji Enstitüsü'nden fizikçi King-Fai Li'nin yönettiği bir ekip, bu olası yıkımı durdurmanın bir yolu olup olmadığını merak etti ve Dünya atmosferinin önümüzdeki birkaç milyar yıla ilişkin modellerini oluşturdu. CO_2 seviyesini sabit tutarak yaptıkları hesaplamalar sonucu ilginç bir durumla karşılaştılar: Değişim, atmosfer basıncının deniz seviyesinde şimdi olduğunun altıda biri kadar olmasını gerektiriyordu. Araştırmacılar *Proceedings of National Academy of Sciences*'da yayımladıkları makalede, bu değişimle biyosferin 1,3 milyar yıl kadar daha var olabileceğini belirtiyor. Araştırmacılar atmosfer basıncındaki düşüşün, atmosferdeki CO_2 ve azotun deniz suyuyla ve okyanus dibindeki kayaçlarla karmaşık etkileşimini etkisizleştireceğini, sonuçta karbonun atmosferden kalıcı olarak uzaklaşmasının yavaşlayacağını ve böylece fotosentezin ömrünün uzayacağını düşünüyor.

Bu basınç düşüşünü sağlamanın bir yolunun, % 78 oranla atmosferin büyük bölümünü oluşturan azotu havadan emecek bir teknoloji geliştirmek olduğu düşünülüyor. Bu durumda hava oksijen bakımından zenginleşecek ama havanın incelmesi gibi bir olumsuzluk doğacak. Bu da, o zaman yaşayacak torunlarımızın, başka insanları ya hasta eden ya da ölümün eşiğine getiren yüksekliklerde rahatça yaşayabilen Nepal'deki Şerpalarla aynı fizyolojiyi geliştirmesini gerektirecek. Yine de konuya olası bir yıkım açısından bakacak olursak, bu şartlar gelecekteki torunlarımıza birazcık nefes aldırabilir!

Atmosferdeki düşük karbon konsantrasyonlarının yol açacağı sonuçlar üzerine çalışan, Stanford'daki Carnegie Enstitüsü'nden küresel ekolog Kenneth Caldeira, araştırmacıların basıncın gezegenimizin uzun vadedeki atmosferik içeriği üzerinde önemli bir rol oynayabileceğine ilişkin ikna edici bir tablo çizdiğini, ancak kendisinin toplam atmosfer basıncının gelecekte nasıl olacağının bilinebileceği konusunda kuşkulu olduğunu belirtiyor.

http://sciencenow.sciencemag.org/cgi/content/full/2009/601/1?rss=1

Süper Hızlı Lazerlerle Enerji Tasarrufu

Osman Topaç

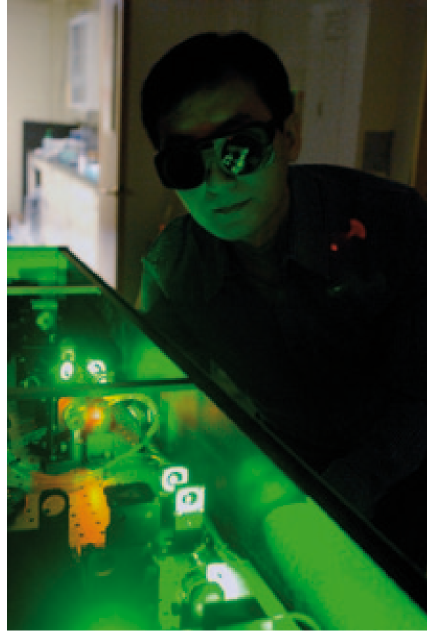
Rochester Üniversitesi'ndeki araştırmacılara göre süper güçlü bir lazer sıradan akkor ampulleri çok daha ekonomik hale getirecek. Bu yeni teknoloji 60 watt'tan daha az elektrikle 100 watt'lık bir parlaklık elde ederek, insan gözüne fluoresan lambaların yaydığı ışıktan çok daha uygun bir ışığı, daha ucuza elde etmemizi sağlayacak.

Lazer teknolojisi, normal bir tungsten ampul telinin yüzeyinde bir dizi nano ve mikro ölçekte yapılar oluşturuyor ve bu yapılar tungstenin daha etkin bir biçimde ışık yaymasını sağlıyor.

Rochester Üniversitesi'nden Doç. Dr. Chunkei Guo "Süper hızlı lazerlerin metalleri nasıl değiştirdiğini zaten araştırıyorduk ve aynı lazeri bir ampuldeki tele tuttuğumuzda ne olacağını merak ettik" diyor ve ekliyor: "Ampulü yaktığımızda, telin sadece lazeri uyguladığımız kısmının daha parlak olduğunu gördük, üstelik ampulün enerji tüketiminde de bir değişiklik olmadı."

Süper ampul teli yapmanın sırrı, tele femtosaniye ($1/10^{-15}$ saniye, yani 32 milyon yıla kıyasla 1 saniye neyse, bir saniyeye kıyasla bir femtosaniye de o kadardır) lazer atımı denilen, çok kısa süreli ve çok yoğun ışın demetleri gönderilmesinde yatıyor. Bu lazer ışını sadece 1 saniyenin birkaç katrilyonda biri kadar bir süre tele tutuluyor. Bu kısa parlama sırasında, Kuzey Amerika kıtasının toplam enerjisi kadar bir enerji, topluiğne başı kadar bir noktaya boşaltılmış oluyor. Bu yoğun enerji boşaltımı, metalin yüzeyinde ışığın telden yayılma etkinliğini çok büyük ölçüder artıran nano ve mikro yapıların oluşmasına neden oluyor.

Guo ve asistanı Anatoliy Vorobyev, 2006 yılında benzeri bir lazer teknolojisini her türlü metali siyahlaştırmak için kullanmışlardı. Bu işlem sonucunda metalin yüzeyinde oluşan yapıların, yüzeye gelen ışınımı, örneğin ışığı, yakalamada



Richard Baker / Rochester Üniversitesi

çok etkin olduğunu gözlemlediler.

Doğada, bir malzemenin aldığı ve yansıttığı ışık oranıyla ilgili olarak "daha çok soğuran, daha çok yansıtır" gibi ilginç bir yasa olmasından yola çıkan Guo ve Vorobyev, siyahlaştırılmış ampul telinin de daha çok ışık soğuracağı ve daha çok ışık yayacağı sonucuna varmış. Guo, bu denemenin başarılı olacağını teorik olarak bildiklerini, ama lambayı açtıklarında lazer ışığını tuttukları bölgeden yayılan ışığın parlaklığı karşısında çok şaşırdıklarını ifade ediyor.

Guo'nun ortaya koyduğu bu yöntemle ampulün parlaklığının artırılmasının yanı sıra ışığın rengini de ayarlamak mümkün. Guo'nun araştırma grubu 2008 yılında, benzeri bir yöntem kullanarak, neredeyse her tür metalin rengini siyahın yanı sıra maviye, altın rengine ve griye çevirmeyi başarmıştı. Guo ve Vorobyev, nanoyapıların büyüklüğünü ve şeklini -yani bu yapıların hangi renkte ışık soğuracağını ve yayacağını- kontrol edebildikleri için, tungsten ampul telinin de ışığın hangi dalga boyunu yansıtacağına karar verebiliyorlar. Guo henüz, örneğin sadece mavi ışık yayan basit bir ampul yapamamış olsa da, yayılan bütün ışık tayfını değiştirip normalde sarımtırak ışık veren tungstenin beyaz ışık vermesini sağlayabiliyor.

Guo'nun araştırma grubu, kısmen polarize ışık yayabilen bir ampul teli de geliştirmeyi başarmış. Bugüne kadar enerji kaybına neden özel filtreler kullanılmadan polarize ışık elde edilmesi mümkün değildi. Birbirine çok yakın, paralel sıralar halinde tasarlanan nanoyapılar sayesinde ise ampul telinden yayılan ışık kısmen polarize oluyor.

Araştırma grubu şu sıralar sıradan bir ampulün başka hangi özelliklerini kontrol edebileceklerini araştırıyor. İşin iyi tarafıysa, femtosaniye lazerler son derece yoğun ışık üretmelerine rağmen, doğrudan duvardaki elektrik prizi kullanılarak çalıştırılabiliyor; dolayısıyla da süreç biraz daha geliştirildiğinde, kullanımları kolaylaşıp yaygınlaşacak.

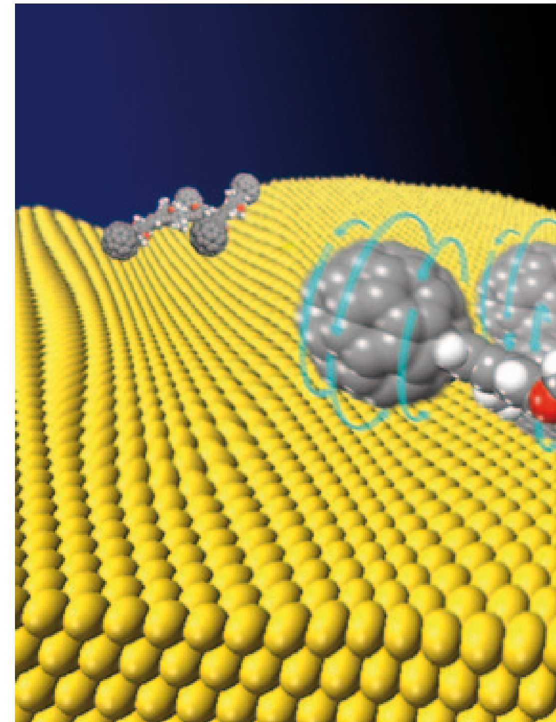
http://www.eurekalert.org/pub_releases/2009-05/uor-rlb052909.php

Yeni Nano Rotorlar

Umut Hasdemir

Çin Bilimler Akademisi ile ortak yürütülen bir araştırmada, sabit bir yüzeyde moleküllerin dönüşlerini gözlemleyen bilim insanları bu hareketin, geleceğin rotor temelli makinelerinin nano boyutlarda geliştirilmesine yapabileceği katkıları araştırıyor.

Araştırma, elektrik motoru ve jeneratör gibi makinelerde önemli



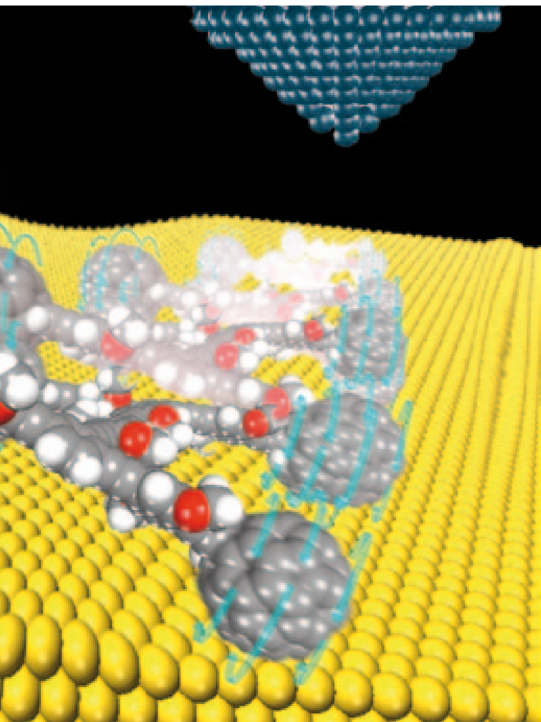
bir rol oynayan dönen manyetik alanlar üzerine odaklanıyor. Atomik ölçekte gerçekleştirilmeye çalışılan bu teknolojinin zorluğu ise bu özelliği moleküler düzeyde taklit edebilmekte yatıyor. Bazı dönen moleküller hâlihazırda belirlenmiş durumda fakat bu moleküller henüz dönen bir manyetik alan yaratmak için kullanılmadı.

Tek bir altın atomunu bağlantı noktası olarak kullanan araştırmacılar ftalosiyanin molekülünün altın bir yüzey üzerinde dönebilmesini sağladı. Yüzeyin en üstünde bulunan bu atom ve ftalosiyanin molekülü arasındaki bağ ise moleküldeki bir azot atomuyla oluşturuldu.

Kimya Profesörü Werner Hofer bunu şöyle açıklıyor: "Moleküler rotor yapmaktaki zorluk, moleküllerin sabit bir bağlantı noktasıyla bağlanmaları gerekmesi ve sabitlemeye çalıştığınız yüzeyle genellikle reaksiyona girmeleridir. Altın yüzeyin moleküllerle etkileşimi çok zayıftır; ayrıca altın yüzeyler tek moleküllerin bağlanması için düzenli bağlantı noktaları sağlar."

"Metalik merkez atomlar altın atomlarının etrafında dönerler. Ftalosiyaninlerin getirdiği avantaj ise merkezin herhangi bir metal atomuyla işlev kazandırılabiliyor olması. Araştırma bundan sonra çok küçük ölçekli dönen manyetik alanların geliştirilmesine yönelebilir."

http://www.eurekalert.org/pub_releases/2009-05/uol-nrc052709.php



nsf

Ağaçtan Plastik Toplamak

İlay Çelik

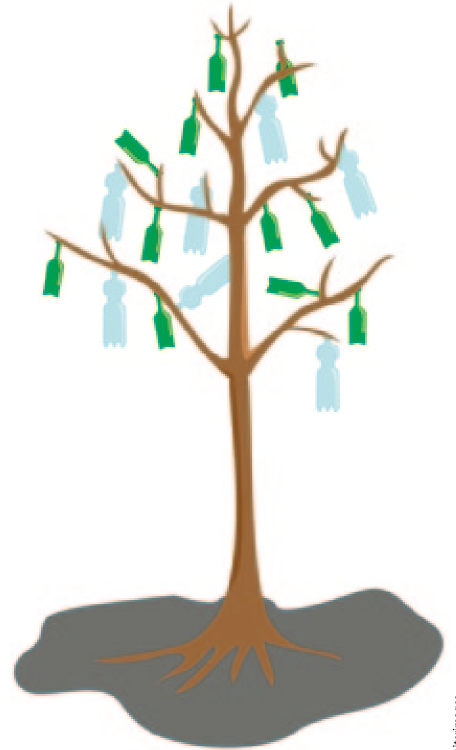
Araştırmacılar bitkileri ham petrolün yenilenebilir ve kirlilik yaratmayan bir muadiline dönüştürebilme konusunda ümitli. Bunu yapabilmek için de bitki biyokütlesini, plastiklerin ve yakıtların bir yapı taşına çevirmenin ucuz ve etkin bir yolunu bulmaları gerekiyor. Yeni bir araştırmada kimyagerler bitkilerdeki en yaygın karbonhidrat olan selülozu HMF denen yapı taşına doğrudan, tek basamaklı bir tepkimeyle çevirmeyi başardılar.

Yapılan araştırma, daha önce ABD Enerji Bakanlığı'nın Pacific Northwest Ulusal Laboratuvarı'nda (PNNL) yapılan, bilim insanlarının selülozdan elde edilen basit şekerlerden HMF ürettikleri bir çalışmaya dayanıyor. Yeni araştırmada araştırmacılar şeker oluşturma basamağını atlamayı ve selülozu doğrudan HMF'ye çevirmeyi sağlayan bir yöntem buldular. Bu basit işlem yüksek verimle HMF üretimi sağlıyor ve ham selüloz kullanımına imkân veriyor.

Kısaca HMF olarak bilinen 5-hidroksimetilfurfural, plastiklerin ve ham petrolden üretilen gazolin ve dizel gibi "biyoyakıtlar"ın yapı taşı olarak kullanılabiliyor. Daha önceki çalışmada PNNL araştırmacıları basit şekerleri HMF'ye dönüştürmek için kimyasal bir madde ile iyonik bir sıvı olarak bilinen bir çözücü kullanmışlardı.

Kimyasal madde, krom klorür olarak bilinen bir metal klorür, şekeri yüksek saflıkta HMF'ye çeviriyordu. Ancak selülozlu biyokütleyi kullanabilmek için araştırmacıların yine de selülozu basit şekerlere ayırmaları gerekiyordu. Çalışmayı yöneten Zhang ve ekibi bu basamağı atlamanın bir yolunu bulmak istediler.

İyonik sıvının avantajı ise selülozu çözebilmesi ki yapraklı sebzeleri pişirenler selülozun ne kadar lifli olduğunu ve zor çözündüğünü bilirler. Katalizör adı verilen maddeler selülozun HMF'ye dönüşümünü hızlandırıyor. İyonik sıvı içerisinde farklı metal klorür katalizörlerini denedikten sonra iyi çalışan bir katalizör çifti keşfettiler: Bakır klorür ve krom klorürden oluşan birleşimle selülozu parçalamayı başardılar, üstelik pek fazla istenmeyen yan ürün de oluşmadı.



Jupiterimages

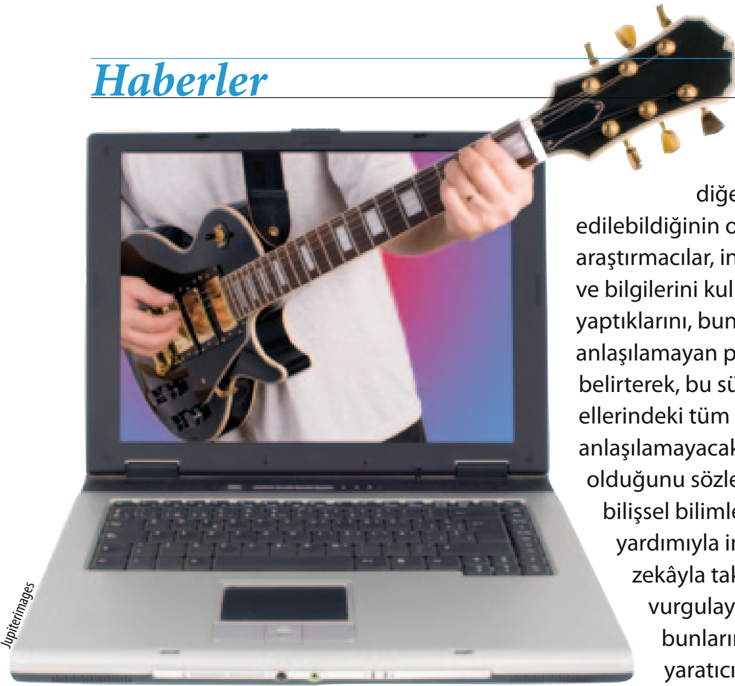
Araştırma ekibi ek deneyler yaparak bu metodu selülozu parçalamanın yaygın bir yolu olan asit kullanımıyla karşılaştırdı. Metal klorür-iyonik sıvı sistemi asitten on kat daha hızlı işledi ve daha düşük sıcaklıklarda çalıştı. Dahası, metal klorür çifti Zhang ve ekibinin incelemekte oldukları bir başka bileşiği, HMF'yi parçaladığı bilinen bir mineral asidi kullanma gerekliliğini de ortadan kaldırdı.

Optimizasyon çalışmaları sırasında istikrarlı olarak yüksek verimle HMF elde edebildiklerini gördüler. Selüloz hammaddedeki şeker içeriğinin % 57'sini bu tek basamaklı işlemle HMF'ye dönüştürmeyi başardılar. Oluşan HMF'nin % 90'ı alınabildi ve son ürün de % 96 oranında saftı.

Üstelik metal klorürler ile iyonik sıvı, etkinliklerini kaybetmeden defalarca kullanılabiliyor. Malzemelerin yeniden kullanılabilmesi HMF üretim maliyetini düşürecek.

Makalenin yazarlarından jeokimyager Jim Amonette bu araştırmayı çığır açıcı olarak niteliyor ve böyle gelişmelerin fosil yakıtlara olan bağımlılığımızı azaltacağını söylüyor.

http://www.eurekalert.org/pub_releases/2009-05/dnnl-ptg051909.php#


Jupiterimages

Telifsiz, Orijinal, Sonsuz...

Özden Hanoğlu

Granada Üniversitesi'nden Miguel Delgado, Waldo Fajardo ve Miguel Molina'nın geliştirmek için yola çıktıkları bilgisayar yazılımıyla artık beste yapma konusunda hiçbir bilgisi olmayan kişilerin de beste yapabilmeleri mümkün olacak.

Araştırmacıların "Inmamusys" (Intelligent Multiagent Music System) adını verdikleri bu yazılım başarılı olursa kamuya açık alanlarda çalınan, duymak zorunda kaldığımız ve sürekli tekrar eden bu müziklerde büyük bir değişiklik olacağa benziyor. Araştırmacılar, kullanıldığı yere göre istenilen duyguyu taşıyabilecek ve her biri diğerinden farklı olacak müzikleri otomatik olarak üretebilecek bir yazılım tasarlamayı hedeflemişler. Böylece kullanıcıya sadece duymak istediği müziğin türüne karar vermek kalıyor.

Inmamusys'un duygu taşıyan parçalar bestelemesini sağlayansa yapay zekâ tekniklerini kullanması. Araştırmacılar, sistemi tasarlayıp geliştirirken kavramların soyut temsilleri üzerinde çalışarak duygu ve hislerin müzikte yansıtılmasını sağlamaya çalışmışlar. Bunun için de iki seviyeli bir "çoklu ajan sistemi mimarisi" kullanmışlar.

Geliştirilen sistemin değerlendirilmesi için yapılan anket çalışmasında, yazılım tarafından bestelenen müziklerin diğerlerinden ayırt edilebildiğinin ortaya çıktığını belirten araştırmacılar, insanların yaratıcılıklarını ve bilgilerini kullanarak beste yaptıklarını, bunun da çoğu henüz anlaşılamayan pek çok süreci kapsadığını belirterek, bu süreçlerin bazılarının da ellerindeki tüm teknolojiye rağmen anlaşılamayacak kadar karmaşık olduğunu sözlerine ekliyorlar. Ayrıca bilişsel bilimlerdeki gelişmelerin de yardımıyla insan davranışlarını yapay zekâyla taklit etmeye çalıştıklarını vurgulayan araştırmacılar, bunların içindeki en zorlu tarafın yaratıcılık olduğunu söylüyorlar.

Inmamusys'u geliştirenler, müziğin çalışma ortamı ve eğlence yerleri gibi yaşamın birçok alanında var olduğunu ve bu müzikler için telif ücreti ödenmesinin gerekli olduğunu hatırlatıyor ve ekliyorlar: "Bu sistem sayesinde dinlediğimiz müziğe ücret ödemek tarihe karışacak."

http://www.eurekalert.org/pub_releases/2009-06/f-sf-eoc060109.php

Öpüşmeye Hazır mısınız?

Özden Hanoğlu

Avuç içinize hohlayarak yaptığınız hızlı bir kontrol bu sorunun cevabını her zaman doğru olarak vermeyebilir. İş görüşmesi öncesinde arkadaşınıza sorarak nefes kontrolü yapabilirsiniz, ama ya çevrede sorabileceğiniz kimse yoksa? Bilim insanları bu derdinize de bir çözüm buldular!

İsrailli araştırmacılar tarafından geliştirilen, cepte taşınabilen bir araç, ağzınızda kötü koku yayan bakterilerin çoğalmakta olup olmadığını hızlıca test edebiliyor. Test aracı üzerindeki pencereye yerleştirilen az miktardaki tükürük, testi gerçekleştirmenizi sağlıyor. Renk değişikliği olmazsa her şey yolunda ancak, mavi renk çıkarsa hemen diş fırçanızı aramaya başlayın. Bu arada araştırmayı gerçekleştiren bilim insanlarının daha önceki çalışmaları olan iki fazlı gargaranın epey ün kazandığını da belirtelim.


Jupiterimages

Bilim insanları şimdiye kadar bakteri popülasyonlarından yalnızca birinin (Gram-negatif olanlar) ağızdaki proteinleri parçalayarak kötü koku yaydığı görüşündeydiler. Yeni yapılan araştırmaysa diğer bakteri popülasyonlarının da (Gram-pozitif olanlar) bu kokuya katkıda bulunduğunu ortaya koyuyor. (Bakterileri ayırmada kullanılan Gram boyama yöntemi onları hücre duvarının özelliklerine göre pozitif ve negatif olarak iki gruba ayırır.)

Araştırmacılar, Gram-pozitif olanların proteinlerin parçalanmasına yardım edecek enzimler salgılayarak Gram-negatif olanlara yardımcı olduğu görüşündeler. Bakterilerin bu faaliyeti tükürük içinde gerçekleşiyor ve nefes kontrolü testi de buna dayanıyor. Gram-pozitif bakterilerin salgıladığı enzimlerin varlığında ortaya çıkan mavi renk, ağzınızın içinde kötü kokuya sebep olacak etkinliklerin yürütüldüğünü haber veriyor.

Test aracının temelini oluşturan yapay biyofilm üzerinde Gram-pozitif ve Gram-negatif bakterilerin oluşturduğu renk farkı çok bariz. Yapay biyofilmin üst tabakasında bakteriler tükürük içerisindeki glikoproteinlerden şeker kalıntılarını temizleyerek kararsız proteinler üretiyorlar. Araştırmacıların dilimize ve ağzımızın iç dokusuna benzettikleri alt tabakada ise Gram-negatif bakteriler yaşıyor.

Geliştirdikleri aracın sosyal hayattaki kullanımı dışında, kişiyi ağız sağlığına dikkat etmeye yönlendireceğini belirten araştırmacılar, diş ipi kullanımını ve diş fırçalamayı teşvik edeceğini de düşünüyorlar. Bir yıl kadar sonra piyasaya sürüleceği tahmin edilen aracın cepte kolayca taşınabilecek boyda örneğin bir sakız paketi büyüklüğünde olacağı tahmin ediliyor.

Bu buluştakine benzer biyoişaretleyicili tanı araçları günlük yaşantımızdaki yerlerini çoktan aldılar: Gebelik testleri ya da cep tipi şeker ölçüm aygıtları bunlardan ikisi. Ağız kokusu kontrolü önemsiz gibi görülebilir ancak tükürük ve biyofilm etkileşmelerini araştırmaya devam eden grubun çalışmaları akciğer kanseri, astım ve ülser teşhisi için ümit vaat ediyor.

http://www.eurekalert.org/pub_releases/2009-05/afot-ayo051809.php

Çernobil ve Bitkiler

İlay Çelik



wikimedia

Dünyanın en korkunç nükleer felaketinin, arkasında çorak bir arazi bıraktığını düşünebilirsiniz. Oysa Ukrayna'daki Çernobil nükleer santralini çevreleyen terk edilmiş sokakları ağaçlar, çalılar ve asmalar bürümüş durumda. Araştırmacılar, Çernobil yakınlarında yetişen soya fasulyelerindeki proteinlerde değişiklikler fark etmişler ki bu da bitkilerin sürekli radyasyon etkisi altında nasıl hayatta kalabildiklerine açıklama getirebilir. Bulgular günün birinde araştırmacıların radyasyona dirençli tarım bitkileri üretmesine yardımcı olabilir.

1986'da Çernobil nükleer santralinde bir reaktör patladı ve çevredeki kırsal bölgeyi radyoaktif maddeler içeren dumanlar kapladı. Bölgede, onlarca yıllık yarı ömre sahip olan sezyum 137 gibi bazı radyoaktif maddelere bugün bile rastlamak mümkün. Yapılan araştırmalarda bölgedeki yaban hayatı üzerindeki tahribatı ortaya koyan veriler elde edildi ve santralin çevresinde 30 km yarıçaplı bir alan yasak bölge ilan edildi. Bu büyük yıkıma rağmen yerel bitki örtüsü hayata dönmeye başladı. Nitra'daki Slovak Bilimler Akademisi'nde bitki biyoloğu olan Martin Hajduch, 23 yıl önce orada öyle bir facia yaşandığının tahmin bile edilemeyeceğini söylüyor.

Hajduch ve ekibi bu bitkilerin radyasyonlu bölgede nasıl hayatta kalabildiğini araştırmaya koyuldu. Ekip, 30 km'lik yasak bölgenin içerisinde, santralin kalıntılarının 5 km yakınına soya fasulyeleri dikti. Aynı zamanda sezyum 137 düzeyinin merkezdekinden 163 kat daha düşük olduğu, santralin 100 km uzağında bir başka yere de aynı fasulyelerden dikildi. Daha sonra olgunlaşan fasulyeler toplanıp içeriğindeki proteinler incelendi.

Radyasyonlu bölgede yetişen fasulyeler protein analizlerinden önce bile sıra dışı görünüyordu. Bu fasulyelerin taneleri diğerlerinin yarısı ağırlıktaydı ve suyu diğerlerinden daha yavaş bir şekilde emiyordu. *Journal of Proteome Research*'ün Haziran sayısındaki makalede bildirildiğine göre bu fasulyeler moleküler açıdan daha da tuhaftı. Yüksek radyasyonlu bölgede yetişen fasulyelerde, ağır metalleri bağlayarak bitkileri koruduğu bilinen sistin sintaz proteininin normal bitkilere kıyasla üç kat daha fazla olduğu tespit edildi. Ayrıca bu bitkilerde, radyasyona maruz kalan insan kanında kromozom anormalliklerini azalttığı anlaşılan betain aldehit dehidrojenaz enziminin % 32 oranında daha fazla olduğu görüldü. Çimlenen tohum için azot sağlayan tohum depo proteinleri de normal fasulyedekilerden farklı yoğunlukta -kimisi daha fazla kimisi daha az- çıktı.

Hajduch'a göre, bitkilerin Çernobil kalıntılarındaki düşük radyasyondan kendilerini koruduğu anlaşılıyor; ancak protein değişimleri ile hayatta kalma mekanizmaları arasındaki ilişki ve bu değişimlerin yeni nesillere geçip geçmediği henüz bilinmiyor. Araştırma ekibi fasulyeleri dört nesil daha incelemeyi planlıyor.

Kolumbiya'daki Güney Carolina Üniversitesi'nden, Çernobil bölgesi yaban hayatı üzerine çalışmalar yapan biyolog Timothy Mousseau bu araştırmanın, özellikle de tüm dünyada nükleer enerjiye yönelik artan ilgi göz önüne alındığında çok önemli bir toplumsal soruna parmak bastığını belirtiyor. Mousseau, eğer araştırmacılar bitkilerin radyasyona nasıl yanıt verdiğini anlayabilirse, nükleer kirliliğe dirençli, hatta nükleer kirliliği temizleyen bitkiler üretmeye başlayabileceklerini söylüyor.

http://sciencenow.sciencemag.org/cgi/content/full/2009/515/2?rss=1





Jupiterimages

Yeni Bir Spor İçeceği: Vişne Suyu

Müge Şener

Yapılan yeni bir araştırma, vişnenin doğal antienflamatuvar (enfeksiyon giderici) gücünün egzersiz sonrası kas ağrılarını hafifletmeye yardımcı olabileceğini ortaya koydu.

Oregon Sağlık ve Bilim Üniversitesi'nde yapılan ve Seattle'da gerçekleştirilen Amerikan Spor Hekimliği Okulu Konferansı'nda sunulan bir araştırmaya göre vişne suyu içmek, koşudan sonra ortaya çıkan ağrıları hafifletiyor. Araştırma, uzun mesafe koşu egzersizi sırasında vişne suyu içen kişilerin içmeyenlere göre egzersiz sonrasında daha az ağrı hissettiklerini gösterdi. Egzersiz sonrası ağrılar kas hasarının ya da güçten düşürücü incinmelerin belirtisi olabiliyor.

Bir bayrak koşusuna katılan ve yaşları 18-50 arasında değişen 60 sağlıklı yetişkinle yapılan bir araştırmada, yarıştan yedi gün öncesinden itibaren ve yarış gününde günde iki kez 0,3 litre vişne suyu içenlerin başka tür bir meyve suyu içenlere göre yarış sonrasında belirgin derecede daha az kas ağrısı hissettikleri görüldü. Koşucular yarışın ardından ağrı seviyelerini 0-10 arası bir aralıkta değerlendirdiklerinde, spor içeceği olarak vişne suyu içenler, ağrı seviyelerini iki birim daha düşük değerlendirdiler; bu da klinik olarak belirgin sayılabilecek bir fark.

Vişne suyunun etkilerini tam olarak anlayabilmek için daha fazla araştırma yapılması gerekse de, araştırmacılar ilk bulguların vişnenin koşucuların egzersiz sonrası enflamasyonu hafifletmek için kullandıkları ilaçların etkisine benzer bir etkisi olduğunu belirttiler.

Araştırmacılardan spor hekimi Kerry Kuehl, koşucuların birçoğu için yarış sonrası tedavinin dinlenme, buz, kompresyon, yükseltme ve bazı yan etkileri olabilecek antienflamatuvar ilaçlardan oluştuğunu, bu yan etkilerin egzersizden önce ilaçlara alternatif olarak vişne suyu gibi doğal maddeler kullanılarak azaltılabileceğini belirtti.

Araştırmacılar vişnenin egzersiz sonrası yararlarının, meyvenin antosiyanin adı verilen antioksidan bileşiklerden doğan antienflamatuvar gücünden kaynaklandığını düşünüyorlar.

Vişne suyunun bu antienflamatuvar gücünden profesyonel ya da amatör olarak spor yapan ve kas ağrılarını hafifletmek için ilaç kullanan milyonlarca kişi faydalanabilir. Aynı araştırmacıların konferansta sundukları ikinci bir araştırmanın sonucuna göre vişne, kalp hastalıklarına ve romatizmaya bağlı olarak gelişen enflamasyonu etkileyebilir ve hatta ağrılı ve kronik bir hastalık olan lif dokusu iltihabı hastalarının kas güçlerini korumalarına yardımcı olabilir.

http://www.eurekalert.org/pub_releases/2009-05/wsw-icj052709.php

Bel Ağrısını Egzersiz Paklar

İlay Çelik

Bel ağrısına hareketsiz kalmak değil aksine daha hareketli olmak iyi geliyor. Alberta Üniversitesi'nde kronik bel ağrısı çeken 240 kadın ve erkek üzerinde yapılan bir çalışmada, haftada dört gün egzersiz yapanların yaşam kalitelerinin daha yüksek olduğu, % 28 daha az ağrı çektikleri ve % 36 daha az zorluk yaşadıkları, buna karşılık haftada sadece iki ya da üç gün egzersiz yapanların aynı gelişmeyi göstermediği gözlemlendi. Alberta Üniversitesi'nde egzersiz fizyolojisi dalında yardımcı doçent olan ve çalışmayı yöneten Robert Kell, genellikle, beli ağrıyanların fazla hareket etmemesi gerektiği düşünülse de elde ettikleri bulgulara göre haftada dört gün ağırlıklarla çalışmanın ağrıyı önemli ölçüde azalttığını ve yaşam kalitesini yükselttiğini söylüyor.



Jupiterimages

Kell, bulgularından bir kısmını 30 Mayıs'ta Seattle Wash'taki Amerikan Spor Hekimliği Okulu Konferansı'nda sundu. Yapılan çalışmada, kronik bel ağrısı çeken 60 kişilik kadınlı erkekli gruplar haftada iki, üç ya da dört günlük programlara uyarak ağırlıklarla egzersiz yaptı, bir grup da hiç egzersiz yapmadı. On altı haftanın sonunda gösterdikleri gelişme ölçüldü. Bel ağrısındaki azalma haftada dört gün egzersiz yapanlarda % 28, üç gün yapanlarda % 18 ve iki gün yapanlarda % 14 olarak ölçüldü. Fiziksel ve zihinsel sağlık olarak tanımlanan yaşam kalitesi ise gruplarda sırasıyla % 28, % 22 ve % 16'lık artışlar gösterdi.

http://www.eurekalert.org/pub_releases/2009-06/uoa-emn060209.php

Yetersiz Uyku Davranış Sorunlarına Yol Açıyor

Adem Uludağ

Finlandiya'da yapılan bir çalışma sonucunda, uyku sorunları yaşamıyor olsalar bile kısa uyku sürelerinin çocuklarda dikkat eksikliği hiperaktivite bozukluğuyla (DEHB) bağlantılı davranışsal belirtilerin görülme riskini arttırdığı öne sürüldü.

Son yirmi otuz yıl içinde uyku süreleri pek çok ülkede kısaldı. Amerika Birleşik Devletleri'nde her üç çocuktan birinin yetersiz uyku nedeniyle sorunlar yaşadığı tahmin ediliyor. Uyku yoksunluğunun çocuklarda yorgunluktan çok davranış bozukluğu belirtileriyle kendini gösterebileceği varsayılıyor, ancak bu varsayımla ilgili araştırma sayısı çok az.

Helsinki Üniversitesi ve Finlandiya Ulusal Sağlık Enstitüsü araştırmacıları, çocuklarda uyku süresinin azaltılmasının, dikkat eksikliği hiperaktivite bozukluğu yaşayan çocuklarda görülenlere benzer davranış bozukluklarına yol açıp açmadığını araştırdılar.

Çalışmaya 146'sı kız ve 134'ü erkek olmak üzere 280 sağlıklı çocuk katıldı. Araştırmacılar ebeveynlerden alınan bilgilerin yanı sıra bileğe takılan ölçüm cihazları kullanarak çocukların uykularını izlediler.

Cihazlarla ölçülen ortalama uyku süreleri 7,7 saatten daha kısa olan çocuklar daha yüksek değerlerde hiperaktivite ve dürtüsel davranış ile dikkat eksikliği hiperaktivite bozukluğu gösterdiler. Ancak bu çocuklarda daha uzun süre uyuyanlara göre yakın dikkat eksikliği değerleri saptandı. Çok değişkenli istatistiksel analizlerde de kısa uyku süreleri, istatistiksel açıdan kayda değer bir hiperaktivite ve dürtüsel davranış habercisi olma niteliğini korudu. Bu analizlerde uyku sorunları da hiperaktivite, dürtüsellik ve dikkat eksikliğiyle ilişkilendirilerek değerlendirildi ve sonuçta kısa uyku ile uyku sorunları arasında belirgin bir etkileşim rastlanmadı.


Jupiterimages

Araştırmacılardan Juulia Paavonen, kısa uyku süresi ile uyku sorunlarının, dikkat eksikliği hiperaktivite bozukluğunun davranışsal belirtileriyle ilişkisi yanında, kısa uykunun bu belirtileri uyku sorunlarından bağımsız olarak arttırdığını göstermeyi başardıklarını belirtiyor.

Bulgular, çocuklarda yeterli uykunun davranışsal belirtilerin önüne geçilmesinde taşıdığı önemi gösteriyor. Yetersiz uykunun davranışlara ve genel performansa etkisinin olumsuz olacağı düşünülse de, aradaki nedensel bağın kanıtlanması için yeni araştırmalar gerekiyor.

http://www.medicalnewstoday.com/articles/147894.php

Balıktaki D Vitamini Beyni Güçlendiriyor

Adem Uludağ

Yeni bir araştırma, uzun süredir "beynin besini" olarak nitelenen balığın, tıpkı sağlıklı koşullarda güneşte kalmak gibi, gerçekten de yaşlı beyinlere iyi geldiğini gösteriyor.

Manchester Üniversitesi'nden bilim insanları, Avrupa'nın çeşitli merkezlerinden meslektaşlarıyla birlikte, yüksek D vitamini düzeylerinin orta ve ileri yaştaki erkeklerde bilişsel işlevlerin artmasıyla ilişkili olduğunu gösterdiler. D vitamini temelde güneş ışığına maruz kalmayı takiben ciltte sentezleniyor ancak yağlı balık gibi belirli gıdalarda da bulunuyor.

Sonuçları *Journal of Neurology, Neurosurgery and Psychiatry* dergisinde yayımlanan çalışma kapsamında yaşları 40 ile 79 arasında olan 3000'den fazla erkeğin bilişsel performansı karşılaştırıldı.

Araştırmacılar dikkat ve işlem hızlarını ölçmek için uyguladıkları basit ve hassas bir nöropsikolojik testte D vitamini düzeyleri yüksek olan erkeklerin sürekli daha iyi sonuçlar elde ettiğini gördüler.

Manchester Aktarımsal Tıp Okulu'ndan Dr. David Lee, yetişkinlerde D vitamini ve bilişsel performans arasındaki ilişkiyi keşfetmeye çalışan önceki çalışmaların yeterli bulgu sağlamadığını ancak kendilerinin, işlem yapma hızındaki düşüklük ile düşük D vitamini düzeyleri arasında önemli bir bağımsız ilişki gözlemlediklerini belirtiyor.

Dr. Lee, ayrıca, geniş bir denek grubunu kapsaması ve deneklerin stres düzeyleri, testlerin yapıldığı mevsim ve fiziksel etkinlik düzeyleri gibi etmenleri hesaba katmasının araştırmalarını güçlü kılan yönler olduğunu söylüyor.

Dr. Lee, "Biyolojik nedenleri henüz anlaşılamasa da, arttırılan D vitamini alımı ile daha hızlı işlem yapma arasındaki ilişki, ilginç şekilde 60 yaşın üzerindeki erkeklerde daha belirgin" diyor. "D vitamininin beyin üzerinde görünürdeki olumlu etkileri, daha fazla araştırma gerektirmekle birlikte, D vitamininin, yaşlanmayla bilişsel performansta yaşanan düşüşleri en aza indirmede potansiyel yararları olabileceğini gösteriyor."

http://www.eurekalert.org/pub_releases/2009-05/uom-vdf051909.php


Jupiterimages

Günde Sekiz Bardak Su Kuralı Uydurma mı?

İlay Çelik



Jupiterimages

Sağlık konusunda bilinçli pek çok insandan şu tavsiyeyi duyarız: "Günde en az sekiz bardak su içmelisin." Üstelik kahve, çay, gazoz ve hatta meyve suyu gibi diğer içeceklerle sulu meyve ve sebzeler sayılmaz.

Suyun yararlı bir şey olduğu yadsınamaz ancak her insanın günde en az iki litre su içmesi gerçekten gerekli mi? Böbrek araştırmaları konusunda uzmanlaşmış ve 45 yılını vücudumuzun su dengesini sağlayan biyolojik sistemi araştırarak geçirmiş olan, Dartmouth Tıp Okulu'ndan emekli fizyoloji profesörü Heinz Valtin'in bu soruya cevabı "Hayır."

Valtin, böbrek taşı ya da idrar yolu enfeksiyonu geçirme eğilimi gibi, özel sağlık sorunları olanlar için çok su içmenin faydalı olabileceğini söylüyor. Ancak 2002'de "günde sekiz bardak" kuralı olarak bilinen genel kural üzerine yaptığı kapsamlı araştırma ve konuyla ilgili iddialar üzerine yaptığı incelemeler sonucu, sağlıklı insanların çok miktarda su tüketmesi gerektiğini destekleyici hiçbir bilimsel kanıt bulamadığını bildiriyor. 2008'de Dan Negoianu ve Stanley Goldfarb, *Journal of American Society of Nephrology*'ye konuyla ilgili bulguları inceledikleri bir derleme yazdılar. Vardıkları sonuç aynıydı: "Fazla miktarda su tüketmenin faydasına ilişkin belirgin bir kanıt yok."

Aslında Valtin, günde sekiz bardak kuralının bir yanlış anlaşılmadan kaynaklanıyor olabileceğini düşünüyor. Şu anda ABD Ulusal Bilimler Akademisi'nin Tıp Enstitüsü'nün bir parçası olan Besin ve Beslenme Kürsüsü, 1945'te bir insanın her 1 kalorilik besine karşılık bir mililitre (bir tatlı kaşığının yaklaşık beşte biri) su tükettiğini ileri sürdü. Bu durumda basit bir hesapla, günde yaklaşık 1900 kalorilik bir beslenme 1900 mililitre suya karşılık geliyordu. Ancak pek çok diyetisyen ve insan önemli bir noktayı gözden kaçırıyordu: Günlük su ihtiyacımızın büyük kısmı yiyeceklerde bulunan suyla karşılanabilirdi.

Kürsü su tüketimi sorununu 2004'te tekrar ele aldı. "Elektrolitler ve suyla ilgili beslenme tercihleri" konulu panelde, yeterli miktarda sıvı alan bir kadının günde yaklaşık 2,7 litre su tükettiği, aynı şekilde yeterli miktarda sıvı alan bir erkeğinse günde yaklaşık 3,7 litre su tükettiğini açıkladı. Görünüşte oldukça yüksek olan bu miktarları kahve, çay, süt, gazoz, meyve suyu, meyveler, sebzeler ve başka yiyecekleri de içeren çok çeşitli kaynaklar oluşturuyordu. Panelde, bir insanın sağlıklı olabilmek için fazladan ne kadar su içmesi gerektiği açıklanmadı ve sağlıklı insanların büyük çoğunluğunun susuzluklarını gidermek için aldıkları sıvılarla günlük su ihtiyaçlarını karşılayabildikleri sonucuna varıldı.

Günde sekiz bardak kuralının savunucuları bazen de susuzluğun yetersiz bir belirti olduğunu ve pek çok insanın kronik olarak susuz kaldığını ve bu yüzden artık susuzluğu bir ihtiyaç belirtisi olarak hissedemediklerini iddia ediyor. Pensilvanya Devlet Üniversitesi'nde beslenme bilimi uzmanı Barbara Rolls araştırmalarında şimdiye kadar insanların kronik olarak susuz kaldığına ilişkin hiçbir kanıta rastlamadığını, her ne kadar bazı ilaçlar susuzluk hissiyle ilgili anormallikler oluşturabiliyor ve yaşlılar susuzluk hissini gençler kadar yoğun hissetmeyebiliyorsa da çoğu sağlıklı insanın yeterince sıvı aldığını belirtiyor.

Günde sekiz bardak taraftarları ayrıca fazla su içmenin kilo vermeye yardımcı olduğunu savunuyor. İnsanların açlık ve susuzluk hislerini karıştırarak aslında sadece susamışken lüzumsuz yere yeme eğilimi gösterdiklerini iddia ediyorlar. Ayrıca su içmenin iştah kestiğini öne sürüyorlar. Ancak Rolls bu iddialara katılmıyor; açlığın ve susuzluğun vücutta ayrı sistemler tarafından kontrol edildiğini, insanların susuzluğu açlıkla karıştırmasının mümkün olmadığını söylüyor. Ayrıca araştırmalarında yemekte ya da öncesinde su içilmesinin iştahı azalttığına dair hiçbir bulguya rastlamadığını belirtiyor. Rolls sadece, sulu besinlerin, tek başına sudan farklı olarak insanların daha az kalori almasına yardımcı olduğunu belirlemiş. Suyun kilo vermeye ancak kalorili bir içeceğe tercih edildiği zaman katkı sağlayabileceğini düşünüyor.

Rolls da Valtin de sağlıklı bir beslenmede suyun bulunması gerektiği, vücudun doğru şekilde işleyebilmesi için suya ihtiyaç duyduğu ve susuzluğun vücuda zarar vereceği konusunda hemfikir. Ancak genel bir kuralın herkes için ideal su tüketimini belirlemesine karşı çıkıyorlar. Rolls su ihtiyacının ortam sıcaklığı, etkinlik düzeyi ve başka etkenlere bağlı olduğunu ve herkese uyan tek bir kural olmadığını söylüyor. Valtin de kimi durumlarda çok fazla su içmenin tehlikeli hatta ölümcül olabileceği uyarısında bulunuyor.

O halde ne kadar su içeceğiz? Tavsiyeleri şu: Bir sağlık sorununuz varsa doktorunuza danışın. Ama sağlıklıysanız Rolls, yemekte bir şeyler içmenizi ve susadığınızda su içmenizi öneriyor. Yani susuzluk hissinizi dinleyin ve fazladan su içmediğiniz için suçluluk hissetmekten vazgeçin.

http://www.scientificamerican.com/article.cfm?id=eight-glasses-water-per-day&print=true

Bel Kalınlığının Gösterdikleri

Sevil Kıvan

Bilim insanları, orta yaşlı ve yaşlı kadınlarda ve erkeklerde bel çevresi genişliğinin artmasıyla kalp yetmezliği riskinin artmasının ilişkili olduğunu buldu.

Kişinin bel çevresi genişliğinin kalp sağlığının önemli bir göstergesi olduğu zaten biliniyordu. Beth Israel Deaconess Tıp Merkezi'ndeki (BIDMC) araştırmacıların yürüttüğü bir araştırmaya göre, orta yaşlı ve yaşlı kadınlarda ve erkeklerde bel çevresi genişliğinin artmasıyla kalp yetmezliği riskinin artması ilişkili.

Araştırmada elde edilen bulgular, vücut kitle indeksi değerinin normal sınırlar içinde kaldığı durumlarda bile bel çevresi genişliğinin artmasının kalp yetmezliğinin bir habercisi olduğuna işaret ediyor.

BIDMC'deki araştırmacılardan Emily Levitan "halihazırda ABD'deki yetişkinlerin % 66'sı ya fazla kilolu ya da obez" diyor. "1989-1999 arasında kalp yetmezliği görülme sıklığının arttığını biliyoruz. Biz de bu değerlere obezitenin bir etkisinin olup olmadığını, varsa bunun nasıl bir etki olduğunu daha iyi anlamak istedik."

Kalbin vücudun ihtiyacını karşılayabilecek kadar kan pompalaya-madığı durumda ortaya çıkan ve hayati tehlike içeren bir hastalık olan kalp yetmezliğine genellikle kişide zaten var olan kalple ilgili hastalıklar, örneğin yüksek tansiyon ve kalp damar hastalıkları neden olur. 65 yaş ve üzerindeki hastaların hastanede tedavi altına alınmasının önde gelen nedeni aşırı yorgunluk, güçsüzlük, yürümekte zorlanma, hızlı veya düzensiz kalp atışları, sürekli öksürük ve hırıltı ile kendini gösteren kalp yetmezliğidir.

BIDMC'deki araştırmacılar İsveç'te iki tıbbi kuruluş tarafından yapılmış, iki ayrı çalışmayı incelemiş. Bu çalışmalardan birinde yaşları 48 ile 83 arasında değişen 36.873 kadının, diğerinde de yaşları 45 ile 79 arasında değişen 43.487 erkeğin boy, kilo ve bel çevresi genişliği değerleri bir anket aracılığıyla kaydedilmiş. 1998 yılının Ocak ayı ile 2004 yılının Aralık ayı arasındaki 7 yıllık dönemde, kadınlardan 382'sinde ilk defa kalp yetmezliği görüldüğü (bunlardan 357'sinin hastanede tedavi gördüğü, 25'inin ise öldüğü), erkeklerin de 718'inde ilk defa kalp yetmezliği görüldüğü (bunlardan da 679'unun hastanede tedavi gördüğü, 39'unun ise öldüğü) bildirilmiş.

Araştırmacıların incelemesi, bu çalışmaya katılan kadınların % 34'ünün fazla kilolu, % 11'inin obez, erkeklerin ise % 46'sının fazla kilolu, % 10'unun obez olduğunu göstermiş.

Levitan'a göre, elde ettikleri bulgular hangi ölçüte göre olursa olsun (vücut kitle indeksi, bel çevresi genişliği, bel-kalça oranı, bel-boy oranı) fazla kilonun kalp yetmezliğinin görülme sıklığının artmasıyla ilişkili olduğunu gösteriyor.

Eldeki verilerin daha da ayrıntılı olarak incelenmesi, vücut kitle indeksi 25 olan (yani normal aralıktaki) kadınlar arasında bel çevresi genişliği diğerlerinden 10 cm daha fazla olanlarda, diğerlerinden % 15 oranında daha yüksek oranda kalp yetmezliği görüldüğünü göstermiş; vücut kitle indeksi 30 olan kadınlarda ise bu oranın % 18'e yükseldiği saptanmış.

Levitan ve ekibi, erkekler arasında (bel çevresi genişliğinden bağımsız olarak) vücut kitle indeksindeki her 1 birimlik artışın % 4 oranında daha fazla kalp yetmezliğine karşılık geldiğini görmüş. Kadınlarda ise vücut kitle indeksi, sadece bel çevresi genişliği en fazla olanlar arasında kalp yetmezliği oranının artmasıyla ilişkiliymiş. Son olarak araştırmacılar vücut kitle indeksi ile kalp yetmezliği vakaları arasındaki ilişkinin yaşla birlikte azaldığını bulmuş; bu da kişi ne kadar gençse kilosunun kalp sağlığı üzerinde o kadar etkili olduğunu gösteriyor.

Levitan'a göre bu araştırma kilonun sağlıklı bir seviyede tutulmasının önemini bir kez daha vurguluyor. "Daha önceki çalışmalarda çeşitli kalp hastalıkları ve bunlarla ilgi sağlık sorunları ele alınmıştı. Bu çalışmaların tümü de, detaylarından bağımsız olarak, aşırı kilonun kişide kalp yetmezliği görülme riskini artırdığını göstermek bakımından tutarlı."

http://www.sciencedaily.com/releases/2009/04/090407174647.htm



Jupiterimages

Bilim ve Teknoloji Yüksek Kurulu Toplantısı Yapıldı


Ali Özdemir

Bilim ve Teknoloji Yüksek Kurulu'nun (BTYK) 19. Toplantısı, Başbakan Recep Tayyip Erdoğan'ın başkanlığında 17 Haziran 2009 tarihinde TÜBİTAK Uzay Teknolojileri Araştırma Enstitüsü'nde yapıldı.

Toplantının açılış konuşmasını Başbakan Recep Tayyip Erdoğan yaptı.

Konuşmasında özellikle Türkiye'deki araştırmacı sayısının artırılmasına değinen Erdoğan, hükümetin Ar-Ge ve yenilik çalışmalarına 2005 yılından itibaren ciddi miktarlarda bütçe ayırdığını, 2008 yılında çıkarılan teşvik yasasıyla özgün teknoloji, araştıma ve yenilik faaliyetlerinin özel sektörün gündeminde de yer almaya başladığını kaydetti.

Başbakan Recep Tayyip Erdoğan'ın ardından söz alan TÜBİTAK Başkanı Prof. Dr. Nüket Yetiş ise sunumunda Bilim ve Teknoloji İnsan Kaynağı, Küresel Mali Krizde Ar-Ge ve Yenilik, Kamu Ar-Ge ve Yenilik Desteklerinin Otomotiv Sektörünün Gelişimine Etkisi, Ar-Ge ve Yenilik İçin Kamu Tedariki ile Ulusal Marker başlıklı konulara değindi.

Prof. Yetiş, 2013'de 150 bin Ar-Ge personeline ulaşmayı hedeflediklerini söyleyerek, Ar-Ge insan gücümüzün mevcut problemlerinin çözülmesi amacıyla yapılan çalışmalar hakkında bilgi verdi.

Prof. Dr. Nüket Yetiş sunumunun bir kısmında ABD Ulusal Bilim Vakfı İnşaat, Makina İmalat Yenilik Bölümü Direktörü iken 1 Ocak 2009'da Bilkent Üniversitesi'nde çalışmaya başlayan Prof. Dr. Adnan Akay'a söz verdi. Prof. Akay konuşmasında Türkiye'ye dönme nedenlerini belirtti ve Türkiye'de ve TÜBİTAK'ta yaşanan olumlu değişikliklerin bu kararı almasında büyük rol oynadığının altını çizdi.

Adnan Akay konuşmasında şunları söyledi: "Yurdumuzda gittikçe ilerleyen araştırma alt yapısı, hem insan kaynakları, hem de fiziki altyapının gelişmesi çok etkileyiciydi. Ama en etkileyici olanı, devletimizin bilim ve teknolojiye verdiği önem ve destek olmuştur. TÜBİTAK, DPT gibi kuruluşların destekleri ve Avrupa Birliği'nin açtığı araştırma yarışlarına girebilme imkanlarının açılması, gerçekten yeni bir ufkun açılması gibi göründü."

Prof. Akay'ın ardından sunumuna devam eden TÜBİTAK Başkanı Prof. Dr. Nüket Yetiş, BTYK'nın bir diğer gündem maddesi olan Üstün Yetenekli Bireylerin Bilim ve Teknoloji Alanlarına Yönlendirilmesi konusunda, Türkiye'de 0-24 yaş aralığında 682 bin üstün zekalı/yetenekli birey bulunduğunun tahmin edildiğini söyledi. Üstün zekalı bireylerin eğitimleri konusunda son yıllarda bütün dünyadaki çalışmalara da değinilen toplantıda topluma yapılan katkılarda üstün zekalı bireylerin payının büyük olduğuna da işaret edildi. Türkiye'de üstün yetenekli bireylerin eğitimini iyileştirmek üzere Milli Eğitim Bakanlığı koordinasyonunda "Üstün Yetenekli Bireyler Strateji ve Uygulama Planı 2009-2013" hazırlanması için çalışmaların başlatılmasına karar verildi. Planın hazırlanmasında bakanlığın yanı sıra Devlet Planlama Teşkilatı, TÜBİTAK ve YÖK de sorumlu kuruluşlar olarak belirlendi.

Prof. Dr. Nüket Yetiş sunumunun "Küresel Mali Krizde Ar-Ge ve Yenilik" konulu bölümünde ise ekonomik kriz ortamını, sürdürülebilir gelişim için bir sıçrama tahtası olarak değerlendirmenin mümkün olduğunu belirtti.

Bilim ve Teknoloji Yüksek Kurulu (BTYK) toplantısında, "Küresel mali krize karşı alınan tedbirler arasında, Ar-Ge ve yenilik alanında uygulamaya alınabilecek ilave eylemlere ayrı bir başlık olarak yer verilmesine" karar verildi.

BTYK toplantısında, Türkiye'nin uluslararası araştırmacılar için daha cazip hale gelmesini sağlamak üzere "Uluslararası Araştırmacılar Koordinasyon Komitesi"nin kurulmasına da karar verildi.


Ali Özdemir

duran.akca@tubitak.gov.tr

Türkiye Florası Projesi

Dünyada zengin bitki örtüsüne sahip sayılı ülkelerden olan Türkiye'nin florasının tüm ayrıntılarıyla, bilimsel nitelikte ilk kez Türkçe olarak yazılması amacıyla Cumhurbaşkanı Abdullah Gül'ün himayesinde, Flora Araştırmaları Derneği çatısı altında büyük bir proje başlatıldı. Türk botanikçilerin bu amaçla biraraya gelerek, 20 cilt tutacak ve 2023 yılında tamamlanacak araştırma ve yazım projesini gerçekleştirmesi hedefleniyor.

Bugüne kadar sadece iki yabancı bilim insanının, biri 19 yüzyılın, diğeri de 20. yüzyılın ikinci yarısında yazdıkları dışına Türkiye'nin florası hakkında Türkçe toplu halde yazılıp basılmış bilimsel kaynak bulunmuyor.

Bütün Avrupa ülkelerinde endemik bitki türü sayısı toplamı 3000 kadarken, ülkemizde bu sayının 3500'e yakın olması Türkiye'nin bu çalışmasının önemini ortaya koymakta. Ayrıca bitkilerin tarım, orman, gıda ve ilaç, kozmetik gibi sanayilerin temel girdilerini oluşturması nedeniyle, bunlar üzerindeki araştırmalar da doğrudan ekonomik gelişmeye katkıda bulunuyor.

Türkiye Florası, Türkiye Cumhuriyeti siyasi sınırları içindeki bitki örtüsünü kapsayan ilk Türkçe temel eser olacak. İlk cildinin 2010 yılı sonunda yayımlanması öngörülen çalışma, her yıl birkaç cilt halinde yayımlanarak devam edecek ve 20. cildi Cumhuriyetimizin 100. yılı olan 2023'de tamamlanacak.

http://www.flora.org.tr



Matematik Eğitimi Öğrenci Kongresi

Kocaeli Üniversitesi Eğitim Fakültesi tarafından 03 - 05 Temmuz 2009 tarihleri arasında "I. Ulusal Matematik Eğitimi Öğrenci Kongresi" düzenlenecek.

Türkiye'deki matematik eğitimi alanında çalışan Lisans ve Lisansüstü öğrencilerini bir araya getirerek; bilgi, deneyim ve bilimsel çalışmaların paylaşılmasına olanak sağlamak amacıyla yapılan kongrede sözlü-poster bildirilere, çağrılı konuşmalara ve sosyal etkinliklere de yer verilecek.

http://www.kouegtmat.org/

1509 Marmara Depreminin 500. Yılı

İstanbul Teknik Üniversitesi Mimarlık Fakültesi, 10 Eylül 1509'da Marmara Denizi'nde Adalar yakınlarında olan büyük Marmara depreminin 500. yıldönümünde bir sempozyum düzenliyor.

10-12 Eylül 2009 tarihleri arasında İTÜ Taşkışla kampüsünde gerçekleştirilecek olan sempozyumda yerli ve yabancı bilim insanları, tarihi Marmara depreminin verileri ışığında olası depremleri tartışacaklar.

http://www.1509.itu.edu.tr

Formula-G ve Hidromobil'09

2009 TÜBİTAK Formula-G ve Hidromobil Yarışları, 8-9 Ağustos tarihleri arasında İzmir Pınarbaşı Yarış Pisti'nde yapılacak. TÜBİTAK Formula-G bu yıl 5. kez, TÜBİTAK Hidromobil ise 3. kez gerçekleştirilecek.

Alternatif enerji kaynakları konusunda kamuoyunda farkındalığı yükseltmek, üniversite öğrencilerini takım çalışmasıyla, başta güneş ve hidrojen olmak üzere temiz ve yenilenebilir enerji kaynaklarıyla





çalışacak ürünler ortaya koymaya özendirmek amacıyla düzenlenen TÜBİTAK Formula-G Güneş Arabaları Yarışı ve TÜBİTAK Hidromobil Hidrojen Arabaları Yarışı, öğrencilerin yaratıcı fikirlerini üretime geçirebilmelerine ve kendilerini geliştirebilmelerine de imkan sağlıyor.

TÜBİTAK Formula-G'ye 40 Güneş Arabası takımı ve TÜBİTAK Hidromobil'e, 21 Hidromobil takımı yarışlara katılmak için başvurdu.

Bilimkurgu Öykü Yarışması

Türkiye Bilişim Derneği (TBD) *Bilişim Dergisi* tarafından ilki 1998 yılında düzenlenen Bilimkurgu Öykü Yarışması için başvurular başladı. Bu yıl yarışmanın konusu "kriz".

Öyküler aracılığıyla krizlerin düşünülmesinin amaçlandığı yarışmada, yazarlar, bilimin "kötüye" kullanılmasından, doğal kaynakların ölçüsüzce tüketilmesinden, belki gelecekte insan, android ve robotlar arasındaki anlaşmazlıklardan ya da umulmadık bir anda yepyeni bir canlı türünün belirmesinden sonra çıkabilecek krizleri ele alabilecekleri gibi dilerlerse kendi kurgularına göre geliştirdikleri krizleri de yazabilecekler.

Son başvuru tarihi 17 Temmuz 2009 olan TBD Bilişim Dergisi Bilimkurgu Öykü Yarışması'nın sonuçları 2 Kasım 2009 tarihinde açıklanacak. Herkesin katılabileceği yarışmada birinci gelecek yarışmacıya dizüstü bilgisayar verilecek. Dereceye giren öyküler TBD web sitesinde, *Bilişim Dergisi*'nde yayınlanacak ve kitap olarak bir öykü seçkisinde yeralacak.

Yarışmaya ilişkin ayrıntılı bilgi için: www.tbd.org.tr

Osman Topaç

Yüz Tanıma Sistemleri



Toshiba

Siz hâlâ bilgisayarınızdaki bilgileri şifre ile mi koruyorsunuz? Bazılarınız parmak izi kullanmaya başlamıştır herhalde. Peki ya şifre ya da parmak izi kullanmak yerine bilgisayarınızdaki bilgilere ulaşmak için ekranınıza bakıp gülümsemeye ne dersiniz? Üzerinde kamera olan pek çok bilgisayara uyarlanan yüz tanıma sistemleri, kullanıcının şifre girmeden bilgisayarını açmasını sağlıyor. Peki bilgisayarlardaki yüz tanıma sistemleri ne kadar güvenli? Gerçek ölçüler büyüklüğünde bir fotoğrafla bilgisayarınızı açabileceğiniz gerçeğinden yola çıkarak çok da güvenli olmadıkları sonucunu çıkarabiliriz.

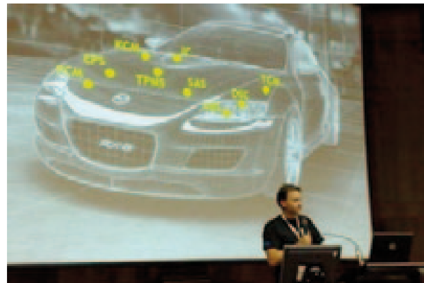
Diğer yandan Toshiba'nın tasarladığı, sürücüler için yüz tanıma sistemi, trafikte ölümcül kazaları önleme kapasitesine sahip bir teknoloji olarak ön plana çıkıyor. Bu yeni teknoloji ile aracın direksiyonu üzerine yerleştirilen bir kamera ile sürücünün yüz ve gözbebeği hareketleri takip edilebilecek. Aynı şekilde aracın önüne yerleştirilen kamera da hareket halindeki aracın yolu üzerindeki nesneleri takip edecek ve bir tehlike karşısında, eğer sürücünün göz bebekleri başka yöne bakıyorsa, sürücüyü uyaracak. Henüz ticari olarak piyasaya ne zaman sürüleceği açıklanmayan bu sistem, aynı zamanda sürücünün göz kırpma frekansını takip ederek sürüş esnasında uyuma belirtisi gösteren sürücüleri uyarabiliyor.

http://www.wired.com/autopia/2009/06/facial-recognition

Bunu Evde Denemeyin: Uzaktan Kumandalı Mazda RX-8





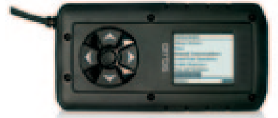


Iphone ve Mazda RX-8. Avustralyalı bir teknoloji delisi olan Jonathan Oxer eline geçen bu iki "oyuncağı" kullanarak ilginç bir uygulama ortaya koymuş. Önce otomobiline Linux işletim sistemi ile çalışan ve 3G mobil iletişim teknolojisi ile internete sürekli bağlı olan GPS donanımlı bir bilgisayar yerleştirmiş. Arabasının bilgisayar kontrollü bütün aksamını bu bilgisayara bağlayan Jonathan Oxer, herhangi bir web tarayıcı üzerinden, arabasını çalıştırabiliyor ve durdurabiliyor, kapısını kilitleyip açabiliyor ve de en önemlisi, arabasının her an nerede olduğunu görebiliyor. Jonathan Oxer, olayı daha da enteresan kılmak için, Iphone'undaki web tarayıcısını kullanarak bir de gösteri yapmış. Bu gösteriyi aşağıdaki web adresinden izleyebilirsiniz. Aslında bu, Jon'un ilk ilginç projesi değil. Yine aynı web sayfasında izleyebileceğiniz daha önceki projesinde Jon, koluna cerrahlar tarafından yerleştirilmiş bir elektronik yonga kullanarak anahtar kullanmadan evinin veya arabasının kapılarını kilitleyip açabiliyor, hatta arabasını çalıştırabiliyor.

http://www.geekmyride.org/wiki/index.php/Jon%27s_RX-8

osmantopac@gmail.com

"Uzay Yolu" Teknolojisi Emrimizde: Voxtec Phraselator®



Dünyanın pek çok ülkesinde birden fazla dil yaygın olarak kullanılıyor. Örneğin Hindistan'da 1500'den fazla dil konuşulmasına karşın, resmi dil sayısı 15 tane ile sınırlıdır. Bu gibi ülkelerde güvenlik güçlerinin en büyük sorunu, dillerini bilmedikleri insan topluluklarına hizmet verirken onlarla ortak bir dil kullanamamaları. Örneğin, 260'tan fazla dilin konuşulduğu ABD'nin Los Angeles şehrinde meydana gelen McArthur Parkı olayında, İngilizce bilmeyen göstericilerle İngilizceden başka dil bilmeyen polis arasında iletişim kopukluğu yaşandı. İngilizce yapılan anonsları anlamadığı için polisin talimatlarına uymayan göstericiler bir arbede yaşanmasına sebep oldu. Bundan ders alan Los Angeles polisi artık bu tür olayların önünü alabilmek için Voxtec Phraselator® P2'den faydalanmaya başladı. Irak'ta bulunan ABD askerleri tarafından da kullanılan bu cihaz, sesli olarak girilen komutları anında yine sesli olarak 40'tan fazla dile çeviriyor. Bu sayede polis anonsları kalabalık bir toplulukta bilinmesi muhtemel dillere çevrilerek anons edilebiliyor. Voxtec Phraselator® P2, çok fazla göç alan yerleşim birimlerinde ya da Hindistan gibi zaten çok sayıda dilin kullanıldığı ülkelerde, güvenlik güçleri, itfaiyeciler ve acil yardım ekiplerinin en çok kullandığı 2500 cümleyi hizmet verilen insanların diline çevirerek önemli bir ihtiyaca cevap veriyor. Voxtec firmasının diğer bir ürünü olan SQU.ID® SQ.200 ise aynı ürünün üste giyilebilen versiyonu. Bu tasarımla hedeflenen ise, acil duruma müdahale eden görevlinin elleri serbest bir şekilde ve dikkati dağılmadan yabancı dilde anons yapabilmesini sağlamak.

http://www.voxtec.com/



{Yakıt Türü=Elektrik}+{Hızı=240 Km}+{Gücü=150 Hp}+{Menzili=240 Km} = Mission One







Elektrikli araç üreticilerinin en önemli hedefi en kısa sürede şarj edilebilen bataryalarla en uzun süre gidebilen araçları geliştirmektir. Mission Motors şirketinin hedefi ise hızlı dolan bir batarya ile en uzun menzile, en hızlı gidebilen bir elektrikli motosiklet üretmek. Mission One adını verdikleri model, şirketin web sayfasında verilen bilgilere göre, 150 beygir gücünde, saatte yaklaşık 240 km hız yapabilen ve dolu bir batarya ile şarj gerektirmeden yaklaşık 240 km gidebilen bir motosiklet. Elektrikli olduğu için doğal olarak benzinli motorlara göre çok daha sessiz olan bu motosiklet, 3-fazlı AC indüksiyon motora ve 240 voltluk bir enerji kaynağı ile iki saatte tam kapasite şarj olabilen sıvı-soğutmalı lityum-iyon bataryalara sahip. Şu ana kadar beş tanesi satılmış olan Mission One modelinin dağıtımına 2010 yılında başlanacağı ve satış fiyatının 69.000 dolar olduğu ilan edilmiş.

http://www.ridemission.com/

Zamanı Esneten Kamera Teknolojisi


JUPITERIMAGES

Geçen sayımızda "En hızlı kamera" başlığı ile 163 nano-saniyede bir görüntü alan yeni bir kamera teknolojisi haberi yer almıştı. Fakat bu kameranın çözünürlüğü sadece 2500 piksel (50×50 piksel) olduğu için henüz bir kullanım alanı bulunmuyor. Diğer yandan, Discovery televizyon kanalında gösterilen Time Wrap adlı programda kullanılan kameralar ise 921.600 piksel (1280×720 piksel) çözünürlükte saniyede 675.000 kare çekebiliyor. Bu çekim hızının ne kadar yüksek olduğu, seyrettiğimiz DVD filmlerin saniyede 30 kareden az olan çekim hızı ile karşılaştırıldığında daha iyi anlaşılabiliyor. Peki bu teknoloji ne işe yarar? Pek çoğumuzun ilgisini çeken ağır çekimde patlayan su dolu balon ya da içinden kurşun geçen elma görüntüleri bu tür kameralarla çekiliyor. Zaten Time Wrap programı da tamamen bu tür görüntülerden oluşuyor. Örneğin, bir sinek kuşunun çiçekten nektar alırken saniyede 70 kez çırptığı kanadını ancak böyle bir kamera ile çekilmiş bir filmi seyrederken net olarak görebilirsiniz. 100.000-130.000 dolara satılan bu kameralarla bir saniyelik görüntüyü birkaç dakikalık muhteşem gösterilere dönüştürmek mümkün. Bu makinelerde çok hızlı DRAM hafızalar ve özel bir kayıt tekniği kullanılıyor. Bu tür kameraların kullanıldığı çekimlerde elde edilmek istenen görüntü 1-2 saniye olmasına rağmen, o 1-2 saniyelik anı yakalamak için çok uzun çekimler yapmak gerekebiliyor. Bu yeni kayıt tekniği sayesinde, çekim esnasında belli bir andan geriye doğru belli bir zaman aralığındaki görüntü saklanırken, daha eski görüntüler otomatik olarak siliniyor. Örneğin, çekim yapan kameraman, kamera kayıtta iken çekmek istediği olayın olmasını bekler. Beklenen olay gerçekleştikten sonra deklanşöre basar ve kamera sadece o olaydan birkaç saniye öncesine kadar olan kısmı saklar. Bu şekilde defalarca çekim yapmaya ya da 100 milisaniyelik görüntü için 20 dakikalık kayıt almaya gerek kalmaz.

http://www.wired.com/gadgetlab/2009/05/highspeed_gallery/

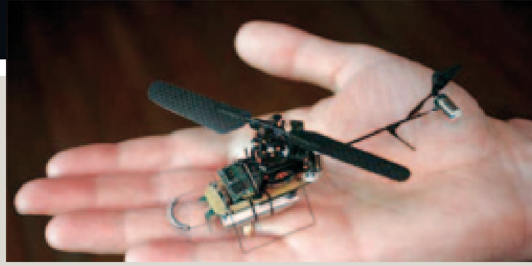
Güneş Enerjili, İnternete Bağlanan Çöp Kutusu



Yenilikçi tasarımların önemli bir kısmı kapsamlı kullanım alanları bulamayabiliyor. Yaklaşan arabanın hızına göre yükselip alçalan hız kesme bariyeri buna bir örnek. Genellikle, çok parlak bir fikir gibi görünen pek çok yenilik, fayda-maliyet oranı açısından, prototip olmaktan öteye geçemiyor. BigBelly® Solar şirketi tarafından geliştirilen çöp kutusu çok uçuk bir fikir gibi görünmesine rağmen, yaygın kullanım alanları bulmaya başlamış bile. BigBelly® CLEAN adı verilen çöp kutuları, üzerindeki güneş panellerinden elde ettiği enerji ile içindeki çöpleri sıkıştırabiliyor. ABD'nin Philadelphia şehrine ilk etapta yerleştirilen 500 güneş enerjili sıkıştırıcılı çöp kutusu, bu sıkıştırma sayesinde, haftada 19 defa yapılan çöp toplama işlemini 5'e indirerek hem çöp toplama maliyetlerini önemli ölçüde azaltıyor hem de daha az dolaşan çöp kamyonları sayesinde yakıttan tasarruf edilmesini ve daha az çevre kirliliği oluşmasını sağlıyor. Bu çöp kutularının başka ilginç özellikleri de var. Kablosuz iletişim teknolojisine sahip olan çöp kutularının dolu olup olmadığı internet üzerinden takip edilebiliyor. Bu şekilde, dolu olan kutuların hemen boşaltılması sağlanıyor ve henüz dolmamış olanları boşaltmak için boş yere eleman ve araç gönderilmesinin önüne geçilmiş oluyor. Normal hacminin beş katı çöp alabilen bu çöp kutuları, petrol fiyatlarının ve personel giderlerinin yüksek olduğu yerlerde kısa sürede kendini amorti edebiliyor. Philadelphia belediyesi, bu akıllı çöp kutuları sayesinde önümüzdeki 10 yıl içinde 10 milyon dolar tasarruf yapmayı planlıyor.

http://www.bigbellysolar.com/

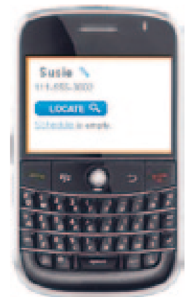
Cep-boy İnsansız Hava Aracı



Norveç merkezli Proxdynamics firması tarafından tasarlanan ve ilk deneme uçuşları başarılı bir şekilde gerçekleştirilen PD-100 Black Hornet, 10 cm'den küçük boyu ve 20 gr'dan hafif ağırlığı ile askeri istihbarat amaçlı üretilen en küçük insansız hava aracı olmaya aday. Piyasaya 2010 yılında sürülmesi planlanan araç, tek kişi tarafından, 1 dakikadan kısa süre içerisinde havalandırılabiliyor ve ulaşılması güç alanlarda personeli tehlikeye atmadan istihbarat toplayabilme imkânı veriyor. 15 cm LCD ekranlı uzaktan kumanda ile kontrol edilen aracın gönderdiği fotoğraflar ve videolar, yine bu kumanda ile kaydedilebiliyor ve gösterilebiliyor.

http://www.proxdynamics.com/products/pd_100_black_hornet/

Yeni Teknolojiler ve Özel Yaşamın İhlali



İlerleyen internet ve bilgisayar teknolojileri, bir yandan bizim ve sevdiklerimizin güvenliği için yeni imkânlar sunarken, diğer yandan da özel yaşamımıza müdahale edilmesi fırsatları doğuruyor. Bunun bir örneği, Amerika Birleşik Devletleri'nde faaliyet gösteren AT&T telefon firmasının cep telefonu abonelerine sunduğu yeni hizmet. "Aile planı" adı altında verilen hizmette, aile bireylerinize bu hizmet kapsamında aldığınız her telefonun nerede olduğunu her an öğrenmeniz mümkün. Eğer bu telefonlarda GPS özelliği bulunuyorsa, telefonun yerini haritada birkaç metrelik bir hata payıyla bulabiliyorsunuz. GPS özelliği olmayan telefonlarda ise bu hata payı birkaç yüz metreye kadar çıkabiliyor. Kullanım alanlarına gelince... Yine hizmetin bir parçası olarak, çocuğunuzun günlük ve haftalık programını gün, saat ve adres olarak sistemin takvimine girdiğinizde, eğer çocuğunuz o tarihte ve saatte olması gereken yerde değilse kısa mesaj veya e-posta yoluyla sistem tarafından uyarılıyorsunuz. Diyelim ki çocuğunuzun saat 9 ile 13 arasında okulunda olması gerekiyor. Okulun adresini ve bu saatleri sisteme giriyorsunuz. Çocuğunuz sabah o saatte okula gitmezse ya da o saatler içinde okulu terk ederse anında size bilgi veriliyor. Her ne kadar güvenlik amaçlı planlanmış bir teknolojik imkân da olsa, böyle bir sistemin özel yaşamı ihlal olarak algılanması her zaman mümkün. Sistemin uygulamasına bu adresten ulaşabilirsiniz: https://familymap.wireless.att.com/finder-att-family/flashDemo.htm

Teknolojinin yaşama getirdiği kolaylıklardan biri olan ve yine özel yaşama müdahale ihtimalini de beraberinde getiren bir başka teknoloji de Google arama motorunun bir parçası olan Google Maps Street View. Bu hizmet ile ABD'nin, Avrupa'nın ve Avustralya'nın pek çok büyük şehrinin sokaklarında görsel olarak gezebiliyorsunuz. Google'a göre, burada gördüğümüz görüntüler, zaten halka açık olan yerler, dolayısıyla da özel yaşama müdahale söz konusu değil. Fakat ünlü Beatles grubunun üyelerinden Paul McCartney aynı fikirde değil. Evinin 360° görüntüsünün internette görülebilir olmasından rahatsız olan Paul McCartney, Google'dan resmin kaldırılmasını istedi ve bunda da başarılı olmuş gözüküyor, çünkü Google Maps Street View onun adresine geldiği zaman fotoğrafın görüntülenemeyeceği mesajını veriyor. İngiltere'de 25 şehrin sokaklarını görüntüleyen Google Maps, insanların şikâyetleri üzerine yüzlerce resmi kaldırmak zorunda kaldı. Hollanda'da ise durum daha da ilginç bir hal alıyor. Evlerinde genelde perde kullanmadıklarını ifade eden bir Hollandalı, Google Maps yüzünden insanların evlerinde bile güvende olamadıklarını belirtiyor, çünkü dikkatli bakıldığında bir evin içini bile görebilmeniz mümkün bu teknoloji sayesinde. Google Maps yetkililerine göre ise, sokaktan geçen bir insanın görebileceği her şeye bakması ne kadar kanunlara uygunsa, görülenlerin fotoğraflarının internette yayımlanması da o kadar uygun. Her ne kadar Google Maps Street View hizmetinin kanunlara uygunluğu İngiltere mahkemelerince onansa da, İngiltere'nin Broughton kasabası sakinleri bu amaçla çekim yapmak üzere kasabalarına gelen aracın kasabalarına girmesini engellemeyi başardılar. Kasaba sakinlerine göre, Google Maps'de, kasabalarının yüzme havuzlu, zengin görünüşlü evlerinin görünmesi, hırsızlık vakalarında artışa neden olmuş. Şu anda bu kasabanın haritasını ve uydu fotoğraflarını görebiliyorsunuz ama sokak fotoğraflarına bakmak istediğinizde ulaşamıyorsunuz. Tabii, kasabanın bu şekilde popüler olmasının hırsızların ilgisini daha çok çekeceği de gözden kaçırılmaması gereken bir gerçek. Google Maps Street View hakkında daha ayrıntılı bilgi için: http://maps.google.com/help/maps/streetview/

Levent Daşkıran

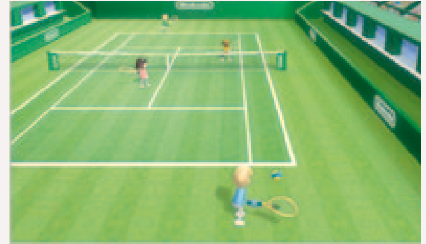
Oyunun Kuralları Değişiyor

Bundan birkaç yıl önce Microsoft ve Sony yeni nesil HD televizyonlarla uyumlu "canavar gibi görüntüye sahip" Xbox 360 ve PS3 konsollarını piyasaya sürerken, uzun zamandır konsol dünyasında kayda değer bir başarı ortaya koyamayan Nintendo, Wii adlı oyun konsoluyla nispeten mütevazı bir çıkış yaptı. Wii diğerlerine oranla öyle süper görüntüler sunamıyordu, ama başka bir iddiası vardı: Gerçek dünyada yaptığınız hareketleri oyuna aktarmak. Yani "Artık oyun oynamak düğmelere saldırmaktan ibaret değil" diyordu Nintendo, "Kalkıp raket sallayacaksın, havada direksiyon tutacaksın, hatta gerekirse hoplayıp zıplayacaksın." Sonuç, Nintendo açısından büyük bir başarıya dönüştü. Çoğu aylarda diğer konsolları satış olarak beşe katlarken, genç yaşında en çok satan konsol rekorunu PS2'den almaya da talip oldu. Bu durum Microsoft ve Sony'nin canını iyice sıkmış olacak ki, ikisi de bu yılki E3 oyun fuarında arka arkaya hareketi oyuna aktaran yeni teknolojilerinin tanıtımını yaptılar. Belli ki 2-3 yıldır bu yeni eğilim karşısında nasıl bir tavır alacaklarını planlıyorlardı. Ortaya koyulan sonuçlar ise insanı gerçekten heyecanlandırıyor.

Bunlardan ilki, Microsoft'un Xbox 360 oyun konsolu için tanıttığı Project Natal adlı sistem. Bu sistem bir grup kamera, kızılötesi algılayıcı ve mikrofon yardımıyla vücudu izliyor ve yapılan tüm hareketleri aynen oyuna aktarıyor. İşin ilginci, Project Natal'ın oyun oynamak için kontrol cihazlarına olan ihtiyacı tamamen ortadan kaldırma iddiasında olması. Top mu gördünüz? Hemen tekmeyi savurun. Araba mı gördünüz? Uzanıp direksiyonunu tutun. Ninja mı gördünüz? Gücünüz yeterse oracıkta pataklayın. Sony ise PlayStation Motion Controller adını verdiği çözümde, tepesinde ışık yanan, harekete duyarlı bir kontrolcüye yer vermiş. Bu kontrolcü oyuncunun eliyle havada yaptığı hareketleri şaşırtıcı bir hassasiyetle konsola aktarırken, konsola bağlı kamera yardımıyla kontrolcüdeki ışık takip edilerek derinlik ayarlaması da yapılabiliyor. Bu sistem nispeten Nintendo'nun Wii'de kullandığı sisteme benziyor, ama belli ki tepkileri ve konumlandırması çok daha hassas. Aslında ben bunlar hakkında buraya ne yazsam eksik kalır, en güzeli tanıtım videolarını izlemek. Project Natal tanıtım videosunu http://getir.net/0gk, PlayStation Motion Controller tanıtım videosunu http://getir.net/0gl adresinden izleyebilirsiniz.



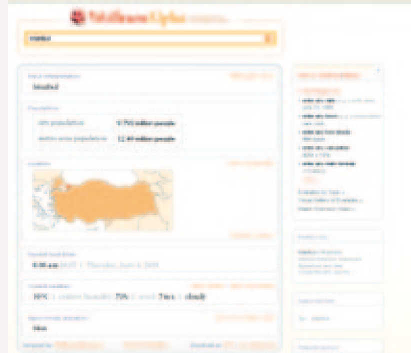
Nintendo'nun başarısının ardından, oyuncunun hareketlerini oyunun bir parçası haline getirme kervanına Sony ve Microsoft da katıldı.



Peki ne zaman? Project Natal için belli bir süre verilmiyor, demek ki biraz daha zamana ihtiyaç var. PlayStation Motion Controller ise yapılan açıklamaya göre 2010'un ilkbahar aylarında piyasada olacak. Öyle görünüyor ki oyun konsolları kendi yarattıkları hareketsizlik sorununu yine kendileri çözme peşinde. Bizse eşofmanlarımızı giydik, bekliyoruz.

İnternette Aramanın Yeni Yolları

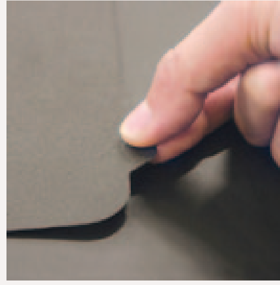
Her ne kadar internette arama yapma konusunda Google'ın üstünlüğü sürse de, bu durum yeni yaklaşımlara engel değil. Geçtiğimiz ay bunlardan özellikle iki tanesi öne çıktı: Biri Wolfram Alpha (http://www.wolframalpha.com), diğeri de Microsoft Bing (http://www.bing.com). Bunlardan Bing aslında Microsoft'un daha önce Windows Live Search olarak adlandırdığı arama motorunun biraz elden geçirilerek yeniden düzenlenmiş hali. Sade görünümü ve Microsoft'un diğer servislerinde görmeye pek alışmadığımız yalın içerik sunumu yaklaşımıyla Google'ın yanında güzel bir alternatif olacağa benziyor. Burada asıl sürprizi yapan ise Wolfram Alpha, çünkü yaklaşımı diğerlerinden çok farklı. Wolfram Alpha'da bir arama yaptığınızda sizi aradığınızı bulabileceğiniz diğer sitelere göndermiyor. Bunun yerine aradığınız şeye dair verileri bir araya toplayıp analiz ediyor ve size doğrudan sonuçları görüntülüyor. Örneğin şehrinizdeki hava durumunu mu merak ettiniz? Size meteoroloji sitesine git diyeceği yerde, o siteye kendi gidip bulunduğunuz yerin hava durumunu alıyor ve anlık durumdan 10 günlük tahmine kadar işinize yarayacak ne bulursa getirip önünüzde sıralıyor. Tarihi bir kişiyi mi arıyorsunuz? Kaç yıl yaşadığı, yaşarken neler yaptığı kronolojik olarak karşınıza geliyor. Bir keresinde önemli bir kişinin ismini aramaya çalışırken ismi herhangi bir genel isim olarak algıladı ve dünyada bu isimde kaç kişi var, yeni doğan çocuklardan yüzde kaçına bu isim koyuluyor, hangi yıllarda bu isim ne kadar popüler olmuş, bu isimdekiler şimdi genel olarak kaç yaşında gibi bilgileri karşıma sıralayıverdi. Gerçekten çok ilginç, denemenizi tavsiye ederim.

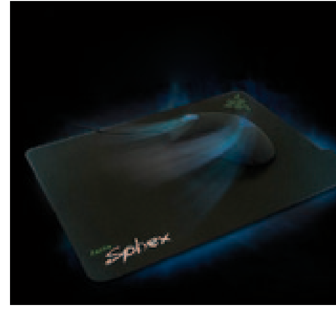


Yeni duyurulan arama motorlarından özellikle Wolfram Alpha'nın arama konusuna yaklaşımı diğerlerinin hiçbirine benzemiyor.

Farenizin Altında Birileri Var

Bugün piyasaya çıkıp şöyle bir dolandığınızda, çoğu yüksek performans gösterme iddiasında olan yüzlerce çeşit fareyle karşılaşabilirsiniz. Aslında optik fareler saçınızda bile gezdirseniz imleci hareket ettirdiği için bu teknoloji yaygınlaştığından beri fare altlıklarının fazlaca bir hükmü kalmadı. Ama fare üreticisi Razer aynı fikirde değil. Aksine, kullandığınız fareden en yüksek verimi alabilmek için sadece içindeki değil, altındaki de önemlidir diyor. Bunun için de Razer Sphex adlı bir fare altlığı üretmiş. İstenen her yüzeye yapışabilen bu altlık, farenin düzgün bir şekilde kaymasını sağlayarak daha hassas bir hareket kabiliyeti sağlıyor. Esas olarak oyunlar için düşünülmüş bir aksesuar olsa da, hassas fare kullanımın önemli olduğu grafik tasarımcılar tarafından da tercih edilebilir. Ayrıca bilgisayarlardaki gelişimin her yerde yaşandığına dair güzel bir örnek. Detayları http://getir.net/0gm adresinde görebilirsiniz.

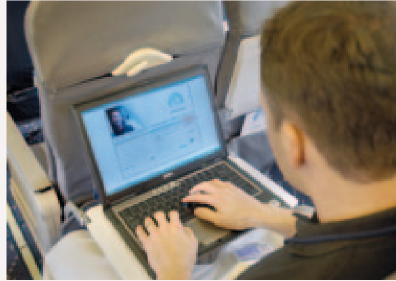




Razer'in yeni fare altlığı, yeni nesil farelerin daha hassas çalışarak performansını artırmasına yardımcı oluyor.

Aç Kalmaya Razıyız Yeter ki İnternet Olsun

Ben her ne kadar teknolojiye yakın olsam da, uçak seyahatleriyle ilgili yukarıdaki gibi bir cümle kurmazdım. Meğer böyle düşünenlerin sayısı azımsanamayacak kadar çokmuş. American Airlines'ın HP sponsorluğunda gerçekleştirdiği araştırmada iş amaçlı olarak sıkça seyahat eden 1500 yolcuya "Size uçak seyahatlerinde vazgeçilmez olan nedir?" diye sormuşlar, % 47'si internet bağlantısı diye cevap vermiş. Soruya yemek olarak cevap verenlerin oranıysa % 30 civarında. Devam edelim; bu kişilerin % 67'sinin en büyük derdi yarı yolda cihazların pilinin bitmesi ve şarj cihazı takacak priz bulamamaları. Bu yüzden uçakta bulunması gereken en önemli teknoloji nedir sorusuna ankete katılanların % 24'ü elektrik prizi diye cevaplamış. Araştırmanın tüm detaylarını http://getir.net/0gn adresinden okuyabilirsiniz. Hadi bakalım, internetin ekmeğe suya tercih edildiği zamanları da gördük sonunda.

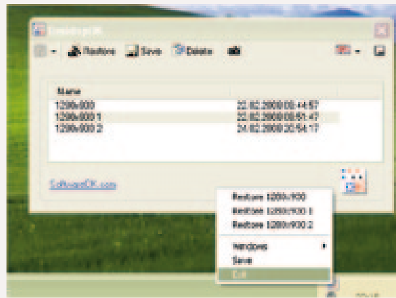




HP sponsorluğundaki American Airlines araştırmasına göre uçakta sık seyahat edenler interneti yemeğe tercih ediyor.

Masaüstü Simgelerinizi Hizaya Sokun

Masaüstündeki simgeleriniz çoğaldıkça doğal olarak bunlarla baş etmek de zorlaşmaya başlar. Çoğumuz böyle durumlarda simgeleri yeniden düzenleyerek ekranın belli bölgelerine dağıtma yoluna gideriz ve kendimizi bu yeni düzene alıştırırız. Gel gelelim, bir nedenle ekran çözünürlüğünün değişmesi veya meraklı minik parmakların bilgisayarınızı kurcalaması yüzünden özenle kurduğunuz bu düzen zaman zaman bozulur. Bu gibi durumlara karşı masaüstü simge düzenini korumak için DesktopOK adlı ücretsiz yazılımdan faydalanabilirsiniz. Sistemde oldukça küçük bir yer kaplayan bu yazılımın yaptığı iş, simgelerinizin masaüstündeki konumlarını kaydetmek ve gerektiğinde tüm simgeleri yeniden eski yerine yerleştirmek. Böylece sebep ne olursa olsun, dağılan masaüstü düzeninizi tek bir tıklamayla eski haline dönüştürebilirsiniz. Program, farklı zamanlarda veya farklı amaçlara yönelik olarak kaydettiğiniz birden fazla masaüstü simge düzenini de sonradan yeniden çağırmak üzere saklayabiliyor. DesktopOK'i indirmek için http://www.software-ok.com/?seite=Freeware/DesktopOK adresini ziyaret edebilirsiniz. Masaüstü için bundan daha fazlasına ihtiyaç duyarsanız, farklı tür simgeleri kendi pencereleri içinde gruplandırmanıza izin veren ve yine ücretsiz bir yazılım olan Stardock Fences'e de göz atmayı unutmayın (http://www.stardock.com/products/fences).



Kalabalık masaüstü simgelerinizin düzenini korumak için DesktopOK adlı yazılımdan yardım alabilirsiniz.

Alparslan Babaoğlu

TÜBİTAK UEKAE Enstitü Müdür Yardımcısı

Kriptolojinin Geçmişi

Bir Şifreleme Algoritması Kullanmadan Önce Son Kullanım Tarihine Bakın!

İnsanoğlunun gizli haberleşmeye gereksindiği günden beri şifreleme teknikleri var. Binlerce yıllık gizli haberleşme tarihinde teknolojinin gelişimiyle şifreleme sistemleri ve cihazlar da değişti. Ancak bir ilke binlerce yıldır geçerliliğini koruyor: Kırılan bir şifre tarihin tozlu sayfalarında yerini alır ve onun yerine daha gelişmişi tasarlanır. Diğer bir deyişle, bir şifre kırılmadığı sürece varlığını korur. Kriptoloji bu ilkeyle gelişerek günümüze kadar geldi. İnsanoğlu Alberti diskini ya da Jefferson tekerleğini binlerce yıl daha önce icat edecek teknolojiye sahipti. Antik çağda şifre kırma teknikleri iki yüzyıl önceki kadar gelişmiş olsaydı, belki şimdi o dönem insanlarının Alberti diskini de Jefferson tekerleğini de kullandıklarından bahsediyor olacaktık.

Anahtar Kavramlar

Askeri haberleşmelerinde kriptografi kullanan ilk ulus Ispartalılardır. MÖ 5. yüzyılda kendi geliştirdikleri bir cihazı tarihin ilk yer değiştirme sistemini uygulamak için kullanıyorlardı.

Şifre anlamına gelen İngilizce "cipher" ve Fransızca "chiffre" kelimeleri bu dillere Arapçadan (cifr ya da cifir) geçmiştir.

Avrupa'da şifre sistemlerinin ilk yaygın kullanım yeri Rönesans'a muhalefet eden Kilise'ydi.



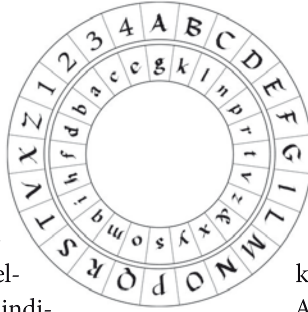
Alparslan Babaoğlu, Manchester Üniversitesi Elektronik Mühendisliği bölümünden 1979'da lisans, 1980'de yüksek lisans derecelerini aldı. TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü müdür yardımcısıdır. Sayısal haberleşme sistemleri, kripto sistemleri, bilgi güvenliği politikaları konularında çalışmaktadır. Bilgi güvenliği konusunda çeşitli kamu kurumlarında seminerler vermektedir.

Bundan 4000 sene önce, Nil nehri kıyısında küçük bir şehir olan Menet Khufu'daki bir kâtip, efendisinin hayatını anlattığı hiyeroglifleri çizerken kriptoloji tarihini başlattığının farkında değildi. Kullandığı sistem modern dünyanın anladığı biçimde bir gizli yazı sistemi olmamasına karşın, metnin rastgele seçilmiş yerlerinde, daha önce hiç kullanılmamış bazı hiyeroglif semboller bulunuyordu.

İlk 3000 yıllık süre zarfında kriptografi sürekli bir gelişim göstermedi. Dünyanın birçok bölgesinde diğer yerlerden bağımsız olarak gelişti ve medeniyetlerin yok olmasıyla birlikte elde edilen birikimler de kayboldu. Antikçağın en ileri medeniyeti olan Çin'de yazının tarihi çok eski olmasına karşın, ideografik yazı (sözleri veya düşünceleri sesleri gösteren harflerle değil çeşitli işaret veya simgelerle yazma sistemi) kullanımına bağlı olarak, bir yazının yazılmasının zaten o yazıyı neredeyse şifrelemekle eş zorluğu olması nedeniyle, kriptografide hemen hemen hiçbir ilerleme kaydedilmedi.

Hrana Janto

Ispartalıların kullandığı kripto cihazı.



Askeri haberleşmede kriptografi kullanan ilk ulus Ispartalılardır. MÖ 5. yüzyılda geliştirdikleri bir cihazı tarihin ilk yerdeğiştirme sistemini uygulamak için kullanıyorlardı. Bu cihaz belli kalınlıkta bir tahta silindirden ve silindirin etrafına eğik biçimde sarılmış papirüs ya da ince, deri bir şeritten oluşuyordu. Gizli mesaj silindir boyunca silindire sarılı şerit üzerine yazılıyor, daha sonra şerit silindirden çözülüyordu. Birbirinden ayrılan harfler yeniden aynı kalınlıkta bir tahta silindire sarılmadıkça hiçbir anlam ifade etmiyordu.

Askeri haberleşmelerde kriptografinin bir diğer önemli kullanımı Roma döneminde oldu. Büyük Roma İmparatoru Julius Caesar, komutanlarıyla kendi geliştirdiği bir yerine koyma sistemini kullanarak haberleşiyordu. Bu sistemde, alfabedeki her harf kendisinden sonra gelen üçüncü harfle (örneğin A, D ile D, G ile) değiştiriliyordu. En temel şifre kırma yöntemlerinden olan ve şifreli metindeki harflerin gözükme sayılarındaki sapmaya dayanan sıklık analiziyle, hiç açık metin olmadan ve hatta şifreleme algoritmasını dahi bilmeden Caesar şifresini kırmak mümkündür. Ancak o dönemde sıklık analizi bilinmiyordu ve Ceasar şifresi Roma ordusunun gereksinimlerini karşılıyordu.

Avrupa'da ortaçağa kadar hiçbir gizli yazışma üzerinde kriptoanaliz yapılmadı. Bu nedenle birkaç istisna durum dışında kriptoanalizle ilgili ciddi bilimsel çalışma olmamış, ancak kriptografi hep var olmuştur.

İlk ciddi kriptoanaliz çalışmaları Araplar tarafından yapıldı. Araplar kriptografi çalışmalarına edebiyatta ve matematikte çağın ilerisinde oldukları MS 600'lü yıllarda başladılar. Şifre anlamına gelen İngilizce "cipher" ve Fransızca "chiffre" sözcükleri bu dillere Arapçadan (cifr ya da cifir) geçmiştir.

Arapların kriptografi konusunda yazdıkları ilk eser, Abdurrahman el-Halil İbn-i Ahmed tarafından MS 718 yılında kaleme alınan *Kitab-ül Muamma* adlı kitaptır. Bu kitapta Abdurrahman el-Halil, Bizans imparatoru tarafından gönderilen Yunanca bir şifreli mektubun çözümünü verir.



wikimedia

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère Karesi

Arapların kriptoloji bilimine en önemli katkısı ise Abdullah Kalkaşandî tarafından 1412'de tamamlanan *Subhu'l A'şâ* adlı 14 ciltlik ansiklopedinin kriptografiyle ilgili bölümleridir. Bu eserde kriptoanalistin ilgilendiği dili bilmek zorunda olduğundan söz edilir ve Arapça'da asla yan yana gelmeyen harflerin bir listesi verilir.

Batı'da günümüze kadar kesintisiz olarak gelen politik kriptografi ortaçağda başladı. Feodal yönetimlerin hâkim olduğu bu dönemde kriptografinin kullanımı ilkel, seyrek ve düzensiz olmakla birlikte sürekli bir gelişim göstermiştir. Avrupa'da kriptografinin ilk günlerinden beri her iki temel yöntem, yani hem kodlar (açık metni oluşturan kelimelerin anlamlı ya da anlamsız başka kelime ya da sayılarla yer değiştirmesi) hem de şifreler (açık metnin belli bir algoritmaya göre şekil değiştirmesi) kullanılmıştır. Şifre sistemlerini yaygın olarak önce Kilise kullandı. 1363 yılında Napoli Kardinali Pietro di Grazie'nin, Papalık ve diğer kardinallerle olan yazışmalarında sesli harfleri kodladığı bir şifre sistemi kullandığını biliyoruz.

Batı dünyasında kriptografinin babası olarak anılan İtalyan Leon Battista Alberti'nin geliştirdiği, iç içe iki diskten oluşan şifreleme cihazında 24 hücre vardı ve cihaz tek alfabeli şifreleme sistemlerinden çok alfabeli şifreleme sistemlerine geçişin ilk örneğini teşkil ediyordu. Kriptoloji tarihi için kritik olan bu başarıdan sonra Alberti kodlamayı ve şifrelemeyi birleştirerek bir başka önemli başarıya daha imza attı: Şifreli kod. Alberti'nin disklerinde harflerle birlikte bulunan dört rakam kodlama amacıyla kullanılıyordu (Bkz. bir önceki sayfa).

Kriptoloji konusunda çağının ilerisinde olan bir başka İtalyan ise Giovanni Battista Porta'ydı. Porta, ünlü kitabı *De Furtivis Literarum Notis*'i yazdığında henüz 28 yaşındaydı. Açık metinde geçen harflerin ikişer ikişer tek bir karakterin yerine geçtikleri, yani iki harfin tek bir karakteri temsil ettiği *digraphic* şifre sistemi Porta'nın buluşudur. Kriptografik sistemler tarihte ilk kez Porta tarafından, harflerin yerlerinin değiştirildiği yerdeğiştirme sistemi ve harflerin birbirinin yerini aldığı yerine koyma sistemi adlarıyla ve bugün de doğru kabul edilen bir sınıflandırmaya tabi tutulmuştur.

1523'te Fransa'da doğan Vigenère'in geliştirdiği ve standart alfabenin kullanıldığı şifreleme sistemi, bugün tüm dünyada Vigenère Karesi olarak bilinir. Sistemin gücü periyodik olmayan anahtar kullanılmasına (anahtar olarak bir kelimenin art arda tekrarının kullanılması yerine rastgele bir cümlenin kullanılması) ve bilinen kripto ihlallerine (bir kripto sisteminin kırılmasına yol açan kullanıcı hatası) meydan verilmemesine bağlıdır. Modern sistemlere örnek olduğu ve temel teşkil ettiği için sistemin nasıl çalıştığı aşağıda açıklanmaktadır.

Açık metin,

t a a r r u z d o k u z d a

Anahtar,

K A L E K A L E K A L E K A

olsun.

Vigenère Karesi'nde şifreleme için küçük harflerle yazılan satır açık metindir. En soldaki sütunsa anahtara aittir. Kapatma işlemi için açık metnin ilk harfi ve ona karşılık gelen anahtar harfi karenin ilk satır ve ilk sütununda belirlenerek, bunların kesiştikleri noktadaki harf bulunur. Bu harf açık metnin ilk harfine karşılık gelen kapalı metnin ilk harfidir. Diğer kapalı harfler de aynı şekilde bulunur. Buna göre şifreli metin,

D A L V B U K H Y K F D N A

olacaktır.

Vigenère'den sonra kriptoloji telgrafın icadına kadar büyük bir ilerleme kaydetmedi. Telgrafın bulunmasıyla, posta işletmelerinde gizli telgrafların görevlilerce açılıp okunması ya da telgraf tellerinin dinlenmesi ile şifreli diplomatik ve askeri haberleşmelerin kolay elde edilebilir olması, hem yeni şifreleme sistemlerinin geliştirilmesini hem de bu sis-

temlerin kriptoanaliziyle ilgili çalışmaların yoğunlaşmasını sağladı.

Vigenère'in yöntemi ya da bu yöntemin değişik biçimlerde kullanımı telgrafın icadından sonra da bir süre devam etti. Ancak, Friedrich Kasiski adlı emekli bir Prusyalı piyade 1863'te bu yöntemi kıran bir test geliştirdi. Literatüre Kasiski testi olarak giren bu analiz yöntemi, şifreli metin içinde beklenenden çok daha sık tekrar eden hecelerin aralarındaki uzaklıklardan anahtarın periyodunu tahmin etmeye dayanıyordu. Kasiski testi özellikle askeri şifre kullanıcılarının paniğe kapılmasına ve yeni şifireleme sistemleri arayışına girmelerine neden oldu. Çözüm, Vigenère'in kırılmasından önce, 1797'de Thomas Jefferson tarafından icat edilen Jefferson cihazıyla geldi. Jefferson'ın cihazı her birinde alfabenin harflerinin yazılı olduğu 36 diskten oluşuyordu.

Charles Wheatstone, 1854'te ilk kez gerçek anlamda *digraphic*, yani harflerin ikişer ikişer şifrelendiği ve sonucun her iki harfe birden bağımlı olduğu bir sistemin haberini verdi. Sistem, Wheatstone tarafından icat edilmişti, ancak arkadaşı Baron Playfair'in adını taşıyordu. Bu sistemin üç önemli özelliği vardı. Öncelikle *digraphic* olduğu için harfler artık kimliklerini kaybetmiş ve tek tek tanınamaz hale gelmiştir. Bu nedenle normal tek alfabeli istatistiksel analiz yöntemleri uygulanamamaktadır. İkinci olarak *digraphic* kodlama istatistik uygulanabilecek mesaj uzunluğunu yarıya indirmektedir. Üçüncü ve en önemli özellikse *digraph*'ların sayısının alfabedeki harf sayısına oranla çok büyük olmasıdır. Bu nedenle dile bağlı karakteristik özellikler çok daha büyük bir sahaya yayılmıştır ve tanınamaz hale gelmiştir. 26 harf yerine 676 *digraph* vardır ve İngilizce'de en çok kullanılan harfler olan *e* ve *t*'nin kullanım oranları sırasıyla yüzde 12 ve 9 olmasına karşılık en çok kullanılan *digraph*'lar olan *th* ve *he*'nin kullanım oranları sırasıyla yüzde 3 ve 2,5'e düşmektedir. Bu özelliklerinden ötürü sistem, zamanında kırılamaz olarak nitelendirilmişti.

Playfair'den sonra kriptoloji biliminde devrim yapmış ve kriptolojiyle matematiğin yakın ilgisini ortaya koymuş bir diğer sistemse Lester Hill'in geliştirdiği Hill sistemidir. Hill, bu sistemin ilkelerini *The American Mathematical Monthly* dergisinin 1929 Haziran-Temmuz sayısında yayımlanan "Cryptography in an Algebraic Alphabet" (Bir Cebirsel Alfabe ile Kriptografi) başlıklı makalesinde ortaya koydu. Hill sistemi, ABD ordusunda sadece üç harf gruplu radyo çağrı sinyallerinin şifrelenmesi amacıyla kullanılmıştır. Ancak, yukarıda da belirtildiği gibi kriptolojinin matematikle olan yakın ilgisinin ortaya konması ve *polygraphic* (birden fazla sayıda açık metin karakterinin şifrelenirken birlikte işleme tabi tutulması) kriptografiyi ilk defa mümkün kılması açısından kriptoloji tarihinde ayrı bir yere ve öneme sahiptir.

Hill, sisteminde anahtar ve açık metin harflerinin sayısal değerlerinin olduğu eşitlikler kullandı. Bu sistemde şifreleme işlemi, denklemlerin çözümlerinin bulunmasından ibarettir. Denklem sayısı, *polygraph*'taki harf sayısına, yani şifrelenirken birlikte işlem gören harf sayısına eşittir. İngiliz alfabesinde 26 harf bulunduğundan ve şifrelerin de çözülebilmesi gerektiğinden Hill tüm işlemlerini MOD-26 üzerinden yaptı. Bu sistem, yalnızca 0'dan 25'e kadar olan sayıların kullanıldığı ve 26'dan büyük her sayıdan, sonuçta 26'dan küçük bir sayı kalana kadar 26'nın çıkartıldığı bir sayı sistemidir.

Hill'in sistemi çok fazla kullanım alanı bulamamış olmasına karşın kriptoloji konusunda çalışanlar üzerinde büyük bir etki bırakır. Çalışmanın güzelliği matematikçileri konuya eğilmeye zorlar. Şifreleme sistemlerinin matematiksel bir biçimde formüle edilmesi, bu sistemlerin zayıflıklarını ve kriptologların sistem tasarımındaki hatalarını ortaya koymaktadır. Daha da önemlisi, kriptoanalistler artık istatistiksel yöntemlerin dışında matematiksel yöntemler de kullanabileceklerini görmüşlerdir.

Bugünkü kriptoloji matematiksel işlemler, matematiksel yöntemler ve matematiksel düşünceyle doyuma ulaşmış bulunuyor. Kriptoloji, uygulamada artık matematiğin bir kolu haline geldi. Bu noktaya gelinmesinde Lester Hill'in katkısı yadsınamaz.

I. Dünya Savaşı sırasında kriptografinin çok yoğun kullanımı ve savaşın haberleşme teknolojisinin ilerlemesine katkısı, savaş sonrasında kriptografinin gelişen teknolojiden daha fazla yararlanmasına neden oldu. Radyo icat edilmişti ve telsiz haberleşmelerini dinlemek artık çok daha kolaydı. Üstelik I. Dünya Savaşı sırasında kriptoanaliz teknikleri de oldukça gelişmişti. Bu nedenle daha güçlü şifreleme sistemlerine gereksinim doğdu. Sonuçta dünyada en çok kullanılacak kriptografik yöntem ortaya çıkacaktı ve bu yöntemle çalışan cihazlar bir sonraki dünya savaşında gizli haberleşmeye yön verecekti: Rotorlu elektromekanik cihazlar...



wikimedia

Jefferson cihazı

Kaynaklar:
Bone, J. V., *A Brief History of Cryptology*, 2005.
Cipher A. D. ve Louis K., *Cryptology: Machines, History, & Methods*, Artech House Cryptology Series, 1989.
Kahn, D., *The Codebreakers: The Story of Secret Writing*, Scribner, 1996.
Menezes, A. J., Oorschot, P. C. ve Vanston, S. A., *Handbook of Applied Cryptography*, CRC, 1997.
Hill, Lester S., "Cryptography in an Algebraic Alphabet," *The American Mathematical Monthly*, Cilt 36, Sayı 6, (Haziran-Temmuz 1929).

Orhun Kara

Dr., TÜBİTAK UEKAE
Başuzman Araştırmacı

II. Dünya Savaşı'ndan Günümüze Kriptoloji: Enigma'dan AES'e Şifreleme

II. Dünya Savaşı'nda Enigma şifreleme cihazını yaygın olarak kullanan Almanlar, savaş sırasında Enigma şifrelerinin Müttefikler tarafından kırıldığının farkında değildi. Yaklaşık yarım milyon Alman mesajını çözen Müttefikler Atlantik'teki Alman "U-boat" savaşında, Normandiya Çıkarması'nda ve Afrika Çöl Savaşları'nda büyük avantaj elde etti. Öyle ki şifre kırma faaliyetlerinin karargâhı haline gelen Londra yakınlarındaki Bletchley Park için Alman Ordusu BBG evi gibiydi!

Anahtar Kavramlar

II. Dünya Savaşı'nda Almanlar Enigma adlı daktilo benzeri şifreleme cihazını yaygın olarak kullandılar. Savaş sonunda ordunun envanterine kayıtlı yaklaşık yüz bin Enigma vardı.

Enigma şifrelerini ilk Polonyalılar kırdı. Ardından İngilizler Bletchley Park'ta Enigma'nın analizi üzerinde çalıştılar. Bletchley Park'ın şifre kırıcıları ülkedeki en yetenekli matematikçilerden, satranç oyuncularından ve bulmaca meraklılarından seçilmişti.

Claude Shannon'ın 1949'da Bell Laboratuvarları'nın teknik dergisinde çıkan "Gizli Sistemlerin Haberleşme Teorisi" adlı makalesi modern simetrik sistemlerin tasarım felsefeleri ve güvenlik modelleri için bir temel oluşturmuştur.

Diffie ve Hellman 1976'da IEEE'nin *Information Theory* dergisinde çıkan "Kriptografide Yeni Yönler" adlı makalelerinde açık bir kanalda iki tarafın nasıl güvenli anahtar paylaşabileceğine dair bir metot önerdiler. Bu makale kriptoloji biliminde çığır açtı.

Rijmen ve Daemen adlı iki Belçikalı kriptoloğun tasarladığı Rijndael adlı algoritma, AES adıyla 1976'da standart olarak kabul edilmiş olan DES adlı algoritmanın yerine standart şifreleme algoritması olarak seçildi.



Bilkent Üniversitesi Matematik Bölümü'nden mezun olan Orhun Kara aynı bölümde yüksek lisans ve doktorasını tamamladı. 2001 ve 2002 yıllarında Fransa'da CNRS'e bağlı IML'de (Institut de Mathématiques de Luminy) Prof. Serge Vladuţ ile çalıştı. Literatürde "reflection attack- yansıtma atağı" olarak bilinen kendine benzeşim atağını buldu. Ayrıca *How to Break Gilbert-Varshamov Bound* adlı kitabın yazarlarındandır. TÜBİTAK UEKAE'de kripto algoritmalarının tasarımı ve analizi üzerinde çalışmaktadır.

Arthur Scherbius adlı bir Alman mühendis XX. yüzyılın başlarında, özellikle bankaların ve iş adamlarının gereksinimleri doğrultusunda ticari gizliliği sağlayacak, pratik, kullanışlı ve güçlü olduğunu düşündüğü rotorlu bir kripto cihazı tasarladı ve cihazına "muamma, bilmece" anlamına gelen Enigma ismini verdi.

Scherbius'un Enigma'sı ilk sürümlerinde hantal olsa da, birkaç sürümden sonra olgunlaştı ve hafifledi. Scherbius, zengin olma hayalleriyle Enigma'ya patent aldı ama iş dünyasından beklediği ilgiyi göremedi. Ticari Enigma İsviçre ordusunda, İspanyol İç Savaşı'nda ve İtalyan donanmasında görev aldı.

Enigma'nın yıldızı asıl Alman donanmasının ilgisiyle parlayacaktı. Almanlar Versay Antlaşması'nın kırgınlığı içinde çoktan yeniden var olma mücadelesine girmişlerdi. Baş döndürücü bir hızla silahlanıyorlardı. Savaş alanında kullanışlı, hafif, ucuz, pratik, anahtar değişimi ve kurulumu kolay bir kripto cihazına ihtiyaçları olacaktı. Enigma tam istedikleri türden bir cihazdı. İlk olarak, o dönemki adı "Kriegsmarine" olan Alman donanması Enigma kullanmaya başladı. Ardından 1930'lu yılların başlarında Alman Gizli Servisi

>>>

"Abwehr", Alman Kara Kuvvetleri "Wehrmacht" ve Alman Hava Kuvvetleri "Luftwaffe", kendi birimlerinde gizli haberleşme için Enigma'yı kullanma kararı aldılar. Enigma II. Dünya Savaşı sırasında Alman ordusunun en yaygın kullandığı şifreleme cihazı oldu. Savaş sonunda ordunun envanterinde kayıtlı yaklaşık yüz bin Enigma vardı.

Enigma yaklaşık 10 kg ağırlığında, daktilo benzeri, rotorlu, elektromekanik bir şifreleme cihazıdır. Tuş takımının hemen üst kısmında 26 harften oluşan ışıklı bir pano yer alır. Operatörün her tuşa basımında ışıklı panoda bir harfin ışığı yanar; bu harf, karşılık gelen şifreli karakter olur.

Enigma'daki matematiksel fonksiyonlar 26 elemanlı harf kümesindeki permütasyonlardı. Bu permütasyonlar ticari Enigma'da üç rotor ve bir yansıtıcıyla ifade ediliyordu. Her bir rotorun bir tarafında 26 pin, diğer tarafında 26 levha bulunuyordu. Her bir pin, rotorun öbür yüzündeki levhalardan birine içerden bir kablo ile bağlıydı. Böylece bir pinden geçen elektrik akımı rotorun diğer tarafında bir levhadan çıkıyor ve bu da 26 elemanlı bir alfabede bir permütasyon ifade ediyordu.

Rotorlar, bir rotorun pinleri diğerinin levhalarına temas edecek şekilde bir çubuk ekseninde, dik konumda yan yana yerleştiriliyor ve en soldaki rotorun levhaları da yansıtıcının pinlerine temas ediyordu. Böylece bir rotorun levhasından geçen elektrik akımı bir sonraki rotorun bu levhaya temas eden pinine atlıyordu. Akım bu şekilde yoluna devam ediyor ve üç rotordan da geçtikten sonra yansıtıcıya ulaşıyordu. Yansıtıcının 26 pini vardı ve kablolarla bu pinler içeriden ikişer ikişer birbirlerine bağlanmışlardı. Böylece bir pinden gelen elektrik akımı diğer bir pinden çıkıp, yansıtıcıya temas eden rotorun başka bir levhasına geri dönüyordu. Akım rotorlardan, rotorların iç telleri üzerinde bu sefer ters yönde ve bambaşka bir yol çizerek tekrar geçiyor ve ardından ışıklı panoya ulaşıyordu. Böylece batarya ile panodaki 26 lambadan biri arasında devre tamamlanmış oluyor ve bu lamba yanıyordu.

Tuşa her basıldığında en sağdaki rotor bir harf kayacak şekilde, yani bir turun yirmi altıda biri kadar dönüyor ve böylece içsel permütasyonlar değişmiş oluyordu. En sağdaki rotor bir tur döndüğünde ortadaki bir harflik, ortadaki bir tur döndüğünde en soldaki bir harflik dönüyordu. Bu da oluşan permütasyonlar kümesinin periyodunun son derece yüksek olmasını sağlıyordu. Bir harfi şifreleme için kullanılan bir permütasyon ancak bütün rotorlar birer tam tur döndüğünde, yani 26x26x26=17576 harf şifrelendikten sonra tekrar kullanılıyordu. Böylece



http://www.nationalmuseum.af.mil



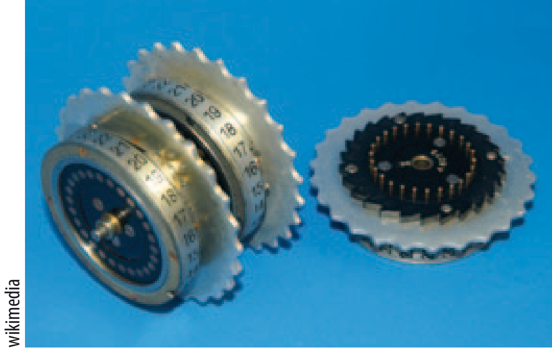
http://www.nationalmuseum.af.mil

Enigma operasyonda. Alman Hava Kuvvetleri askerleri Enigma'nın başında. Bir operatör şifreleme yaparken (şifre çözerken) diğer operatör kaydediyor.

pratikte her harf şifrelenişinde farklı bir permütasyon kullanılmış oluyordu.

Enigma permütasyonların özelliği *involüsyon* olmalarıydı, yani harfler karşılıklı olarak birbirlerine gidiyorlardı. Örneğin A harfi Z'ye gidiyorsa Z harfi de A'ya gidiyordu. Bu durum yansıtıcının da *involüsyon* olması ve yansıtıcıdan sonra rotorların belirlediği permütasyonların ters yönde ve ters sıra ile tekrar uygulanması sayesinde oluyordu. Böylece cihazın aynı kurulumuyla şifre çözme de kolayca gerçeklenebiliyordu.

Alman ordusunda kullanılan Enigma'ya ticari Enigma'lardan farklı olarak bir de "steckerbrett" denilen fişleme tablosu eklenmişti. Hemen tuş takımının ardında yer alan bu tabloda 26 harf oyuğu bulunuyordu. Bir fişin bir ucu bir harfin oyuğuna, diğer ucu da başka bir harfin oyuğuna takıldığında bu iki harf yer değiştirmiş gibi davranıyordu. Örneğin A harfi ile Z harfi bir fiş ile bağlandığında, A harfi Z, Z harfi de A gibi davranıyordu. Operatör A harfine bastığında sanki Z harfine basılmış gibi elektrik akımı rotorlara iletiliyordu. Şifre çözme işleminin de aynı olması açısından, cihazın ürettiği permütas-


wikimedia

Enigma'nın rotorları. Yan yatmış rotorda 26 pin ve öndeki rotorda 26 levha gözükmektedir.

yonları *involüsyon* yapmak gerekiyordu. Bu yüzden akım son olarak ışıklı panoya gelmeden fişleme tablosundan tekrar geçiyordu.

Fişleme tablosunda çiftler halinde hangi harflerin kablolarla birbirlerine bağlanacağı anahtar bilgisiydi ve bu da tek tek deneme yoluyla anahtarı bulmayı pratikte imkânsız kılacak kadar çok kombinasyon sunuyordu. 26 harften 13 çift $26!/(13!\times2^{13})$ farklı yolla oluşturulabilir ki bu da 13 basamaklı bir sayıdır.

Ticari Enigma'dan farklı başka bir uygulama olarak Almanlar beş rotor bulunduruyor ve üçünü seçerek kullanıyorlardı. Bu da anahtar bilgisinin bir parçasıydı ve sisteme 60 kat karmaşıklık getiriyordu.

Ticari Enigma'yı Polonyalılar ve İngilizler kırdılar. İngilizler şifre kırma faaliyetlerini kurumsal hale getirmek için GC&CS (Government Code and Cipher School - Devlet Kod ve Şifre Okulu) adlı bir yapı oluşturmuştu. GC&CS İspanyol İç Savaşı'nda kullanılan Enigma şifrelerini çözmeyi başarmıştı, ama 1930'lu yıllarda Alman Ordusunun Enigma'sı İngilizler için hâlâ bir muammaydı.

Alman Enigma'sını ilk kıranlar Polonyalılar oldu. Polonyalılar yaklaşan Alman tehlikesini sezmiş olacaklar ki daha 1930'lu yılların başlarında, Varşova yakınlarında en iyi matematikçilerin toplandığı bir şifre kırma okulu kurdular. Bu okulda en başarılı üç matematikçiyi -Marian Rejewski, Henryk Zgalski ve Jerzy Rozicki- Enigma'yı analiz etmek üzere çok gizli bir görevle Biuro Szyfrom'a (Şifre Bürosu) aldılar. Bu üç matematikçinin Biuro Szyfrom'da yoğun çalışmaları kısa sürede meyvelerini verdi ve Polonyalılar Enigma'yı kırmayı başardı.

Hans-Thilo Schmidt adlı bir Alman casusun Fransızlara aktardığı bilgiler Enigma'nın analizinde Polonyalıların oldukça işine yaradı. Ayrıca bir başka gelişme Polonyalıların ekmeğine yağ sürecekti. Alman hükümeti büyük bir hata yaparak bir diplomatik Enigma'yı Berlin'den Varşova'daki büyükelçiliğe sıradan bir kargo gibi gönderdi. Bunu fark eden Polonyalılar Enigma'yı ele geçirdiler ve iki gün boyunca kurcaladılar. Cihazların iç tel sistemlerini inceleyip fotoğraflarını çektiler. Ardından hiçbir şey olmamış gibi paketleyip Alman Büyükelçiliği'ne teslim ettiler. Almanlar durumun farkına varmadı ama Polonyalılar sistemle ilgili her şeyi öğrenmişti. Hatta iki tane kopya Enigma dahi ürettiler.

Biuro Szyfrom'da özellikle Marian Rejewski, Enigma'nın analizinde oldukça başarılı sonuçlar elde etti. Enigma'nın iç sisteminin birçok permütasyonu üretemeyeceğini keşfetmişti. Sonuçta rotorların oluşturduğu permütasyonları olası adaylar arasından eleme yoluyla bulan bir cihaz geliştirdi. Cihaza "bombe" adı verilmişti. Bu, tarihte bilinen ilk kriptoanaliz cihazıydı ve altı Enigma cihazını aynı anda taklit edebiliyordu. Bir rivayete göre, cihazdaki Enigma rotorlarını taklit eden yassı toplar o dönem Polonya'da yaygın olan ve bombe adı verilen tatlılara benzediği için cihaza bombe adı verilmişti. Başka bir rivayete göre ise cihazın ismi bu topların çalışırken, düşen bombaların ıslıkları gibi ses çıkarmalarından geliyordu.

Bombe cihazlarını Polonya'nın radyo fabrikası olan AVA şirketi üretiyordu. 1939 sonbaharında Almanların Polonya'yı işgalinden hemen önce kriptoanaliz faaliyetleri durduruldu ve Biuro Szyfrom lağ-


Visual Photos

Alman donanması tarafından 1942'den sonra kullanılan ve M4 adı verilen dört rotorlu Enigma.

>>>

vedildi. Polonyalılar hiçbir kanıt bırakmamak için bütün çalışmaları ve bombeleri yok ettiler. Bu yüzden maalesef günümüze Polonya bombesinden bir örnek, hatta bir fotoğraf dahi kalmamıştır.

Alman işgaliyle birlikte Polonyalı kriptoanalistlerin birçoğu Fransa'ya veya İngiltere'ye kaçtı. Enigma'nın kriptoanalizi artık İngilizlere kalmıştı. İngilizler 1930'lu yıllarda bu konuda Polonyalılardan çok şey öğrendiler. GC&CS, karargâhını 1939'da Londra'dan yaklaşık 90 km uzakta bir banliyö kasabası olan Bletchley'de kurdu. Kriptoanaliz çalışmalarını başlangıçta küçük ve mütevazı bir ekip yapıyordu. İşler büyüdükçe ekip de genişledi. Öyle ki savaşın sonuna doğru yaklaşık 8000 kişilik dev bir kriptoanaliz ordusu harıl harıl Alman şifrelerini çözmekteydi.

Bletchley Park'ta çalışan şifre kırıcılar ülkedeki en yetenekli matematikçilerden, satranç oyuncularından ve bulmaca meraklılarından seçilmişti. Bu isimler arasında özelikle Alan Turing ve Gordon Welchman dikkat çekiyordu. Turing, Polonya bombesi üzerinde yoğun bir çalışmaya daldı ve sonunda kendisi de bir Enigma şifre kırma cihazı geliştirmeyi başardı. Cihazın çalışma ilkesi Polonya bombesinden çok farklı olmasına karşın bu cihaza da bombe ismi verildi.

İngiliz bombeleri bir ton ağırlığında ve üç yatay bataryadan oluşan devasa makinelerdi. Bataryalar, her bir sırası Enigma rotorlarını taklit eden dönen toplardan oluşan üç sıra teşkil ediyordu. En hızlı dönen top Enigma'nın en soldaki rotorunu temsil ediyordu ve saniyede iki tur atıyordu. Bir Enigma aynı hızda çalıştırılmak istense saniyede 52 tuşa basmak gerekecekti! Üstelik bir bombe üzerinde onlarca Enigma simülasyonu aynı anda paralel çalışıyordu.

Bu devasa kriptoanaliz makineleri çok hızlı onlarca Enigma gibi davransa da makinelerin anahtarları tek tek deneyerek bulmaları yıllar alacak bir işlemdi. Bombelerin taramaları aslında Turing'in keşfettiği Enigma'nın bir zayıflığını kullanıyordu ve aday permütasyonlar şaşırtıcı bir hızla eleniyordu.

Bombeler BTM (British Tabulating Machine-İngiliz Tablolama Makinesi) fabrikası tarafından büyük bir gizlilikle üretiliyor ve Bletchley Park'a getiriliyordu. İlk iki bombe 1940'ın Mart ayında göreve başladı. İngilizler savaş sonuna kadar 200'den fazla bombe ürettiler ve bu makinelerle neredeyse yarım milyon Alman mesajını çözmeyi başardılar.

Y istasyonları adı verilen dinleme istasyonlarında toplanan sinyallerden şifreli metinler çıkarılıyor ve Bletchley'e gönderiliyordu. Bletchley'de çözülen metinler sınıflandırılıyor ve kurmaylar tarafından değerlendirmeye alınıyordu. Almanlar günlük anahtar kullanıyorlardı. Genellikle gece yarısı değiştirilen anahtarlar, öğleye doğru Bletchley'de İngilizlerin eline geçmiş oluyordu.

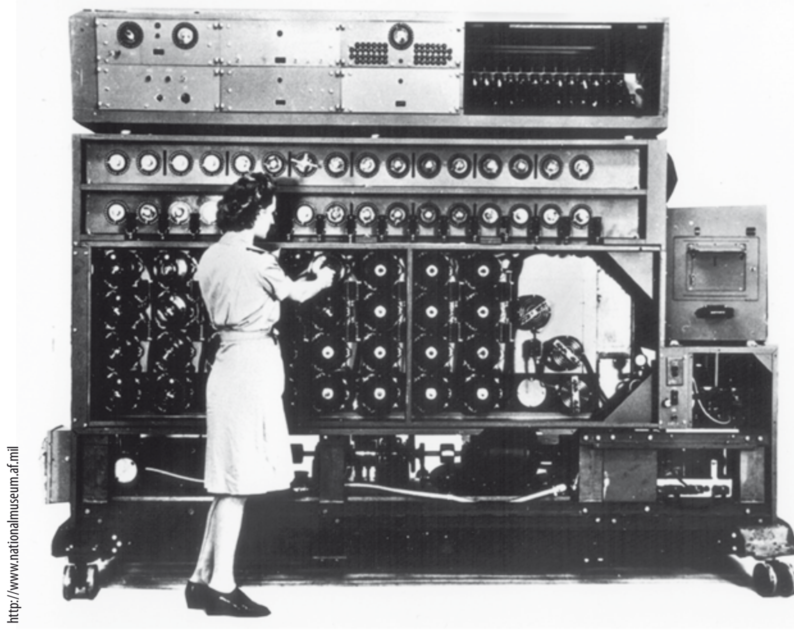


Visual Photos

Enigma'nın rotorları.

İngiliz bombesi "bilinen açık metin atağı" uyguluyordu. Dolayısıyla İngilizlere Y istasyonlarında topladıkları şifreli metinlerin bir kısmına karşılık gelen açık metinler gerekiyordu. Ancak açık metin elde etmek onlar için hiç de zor olmadı. Sabit hava raporları, mesajların belli yerlerinde geçen "cevap bekleniyor", "derhal" gibi tekrar eden sözcükler, kalıplaşmış askeri terimler, mesajların standart başlangıç ve bitiş şekilleri, test mesajları ve içi doldurulan matbu formlar İngilizlere kolayca açık metin sağlıyordu.

Bombe üretmek oldukça pahalıya mal oluyordu. Üstelik 1942 başlarında Alman donanması Enigma'ya bir rotor daha eklemişti. M4 kodlu bu Enigma'lara Bletchley sakinleri "shark" (köpek balığı) adını verdiler. Çözülemeyen "shark" kodları Bletchley'i zor durumda bırakıyordu. İngilizler ABD'den yardım istediler. Amerikalılar da 1942'nin sonlarında bombe üretmeye başladılar. Onların



http://www.nationalmuseum.af.mil

WAVES adı verilen operatörlerce kurulan ABD donanma bombesi. Bu dev makinelerde Turing'in Enigma'ya karşı geliştirdiği atak gerçekleniyordu.

bombesi 2,5 ton ağırlığındaydı ve daha hızlı çalışıyordu. Ürettikleri ilk iki bombeye Âdem ve Havva adını koydular. İlginçtir, projenin başında Joseph Desch adlı bir Alman vardı. Ar-Ge çalışmaları NCML'de (Naval Computing Machine Lab-Donanma Hesaplama Makineleri Labaratuvarı) yapıldı ve bombeler NCR (National Cash Register-Ulusal Kasa) firmasında üretildi (Bir ATM cihazından para çekerken cihazın bir köşesinde NCR yazısı dikkatinizi çekmiş olabilir. NCR aynı zamanda ATM de üretiyor). Amerikalılar savaş sonuna kadar yüzden fazla bombe ürettiler.

Alan Turing ve ekibi M4 Enigma'sının analizleri üzerine yoğun çalışmalarının semeresini görmeye başladı. 1942'nin sonbaharına doğru Bletchley Park'ta artık köpek balığı kodları çözülebiliyordu. ABD bombeleri de köpek balığı kodlarını okuyabiliyordu.

Bletchley Park'ta sadece Enigma kodları çözülmüyordu. Yüksek rütbeli Alman askerlerin ve kurmayların kullandığı Lorenz SZ-40 Schlüsselzuzatz eklenti şifresi tam 12 rotorluydu ve teleyazıcı devreleri için kullanılıyordu. Bletchley'de Lorenz ile gönderilmiş şifrelere "tuna kodu" deniliyordu. Tuna kodları John Tiltman ve William Tutte tarafından analiz edildi ve kırıldı. Sonuçta, Hitler'in haberleşmesi bile dinlenebilir hale geldi. Bletchley'de tuna kodlarını çözmek için Colossus adı verilen ve delikli şerit kâğıtlar yardımıyla programlanabilen dev cihazlar geliştirildi.

Bletchley Park projesinin başında, büyük bir gizlilik içinde yapılan şifre kırma işlemlerine "ultra sır" adını veren dönemin başbakanı Churchill vardı. Bu yüzden projeye "Ultra Projesi" dendi. Bletchley Park'ta olup bitenler o kadar gizli tutuluyordu ki "ultra" bilgileri kullanılırken kaynağın "boniface" (hancı) kod adlı bir casus olduğu söyleniyordu.

Ultra Projesi Atlantik'te, Afrika Çöl Savaşları'nda ve Normandiya Çıkarması'nda Müttefiklere önemli avantajlar sağladı. Birçok tarihçi Bletchley'deki şifre kırıcılar sayesinde savaşın en az iki yıl kısaldığı konusunda hemfikir. Müttefikler Atlantik'teki Alman denizaltılarının yerlerini kolayca saptadılar. Ayrıca, I. Dünya Savaşı'nda efsane olmuş Alman komutan Mareşal Rommel, şifre kırıcıların da etkisiyle Afrika'daki savaşı kaybetmişti. Bletchley Park, Akdeniz'deki Alman mühimmat gemilerinin yerlerini gerçek zamanda saptayabiliyordu. Üstelik Almanların savaş planları anında İngiliz Mareşal Montgomery'in önüne seriliyordu. Öyle ki Hitler'in Rommel'e gönderdiği bazı mesajlar gecikebiliyor ve bu mesajlar Rommel'e ulaşıncaya kadar, çoktan Bletchley Park'ta çözülmüş ve Montgomery'e iletilmiş oluyordu.

Şifre kırıcıların elde ettiği bilgiler Normandiya Çıkarması'nda General Eisenhover'ın -kendi ifadesiyle- işini çok kolaylaştırmış ve birçok askerinin hayatını kurtarmıştı.

Ultra Projesi'nin başarısında Bletchley Park'taki çok geniş ve yetenekli bir kadronun hummalı çalışması ve projenin iyi yönetilmesi kadar, Enigma'daki analitik zayıflıklar ve operatörlerin yaptığı kripto ihlalleri de (kripto güvenliği için uyulması gereken kuralların göz ardı edilmesi) etkili olmuştu. Tarih ders alınacak olaylarla doludur. Bletchley Park buna güzel bir örnektir.

Enigma gerçekten de çağına göre son derece üstün bir şifreleme makinesiydi. Ancak Alman ordusu Enigma'yı kullanmadan önce detaylı test ve analizlerden geçirmedi. Böylece kolayca önlem alınabilecek zayıflıklar gözden kaçmış oldu. Almanlar Enigma'ya aşırı güvendiler ve Enigma trafiğinin dinlenmesinin imkânsız olduğunu düşündüler. Düşmanlarının kriptoanaliz kabiliyetlerini ve hesaplama güçlerini küçümsediler. Ancak bu aşırı güven Almanlara pahalıya mal oldu.

II. Dünya Savaşı'nın bir başka büyük kriptoanaliz projesi de ABD donanmasının yürüttüğü "Magic Projesi"ydi. Japonların diplomatik amaçlı kullandıkları rotorlu bir şifreleme cihazı olan "Purple", ABD kriptoanalistleri tarafından kırıldı. Gerçi Japon ordusu askeri gizli haberleşmelerin diplomatik cihazlarla yapılmamasına özen gösteriyordu ama ABD'li kriptoanalistler İngilizlerin de yardımıyla Purple'la şifrelenmiş iki önemli mesajı açmayı başardılar. Bunlardan biri Berlin'deki Japon büyükelçi-

sinin, Hitler'le görüşmelerini uzun bir rapor halinde, Purple'la Japonya'ya gönderdiği mesajdı. Diğer mesaj ise Pearl Harbor saldırısından önce Japon hükümeti tarafından ABD'deki Japon Büyükelçiliği'ne gönderilen bir dizi acil talimat listesiydi. Bu talimatlardan özellikle iki tanesi dikkat çekiciydi: ABD ile bütün ilişkiler derhal kesilecekti ve ABD karasularındaki bütün Japon gemilerinin acilen ABD karasularını terk etmesi sağlanacaktı.

II. Dünya Savaşı Sonrasında ve Günümüzde Kriptoloji

II. Dünya Savaşı'nın ardından kriptolojinin artık bir bilim olma yolunda emin adımlarla ilerlediğini görüyoruz. Claude Shannon'ın 1949'da Bell Laboratuarları'nın teknik dergisinde çıkan "Gizli Sistemlerin Haberleşme Teorisi" adlı makalesi modern simetrik sistemlerin tasarım felsefeleri ve güvenlik modelleri için bir temel oluşturmuştur.

1970'li yılların başlarında, içlerinde Feistel ve Coppersmith'in de olduğu IBM mühendisleri tarafından tasarlanan LUCIFER adlı blok şifreleme algoritmasının Shannon'un 1949'da ortaya koyduğu ilkeleri taşıdığını görebiliriz. Bu algoritma daha sonra NSA (National Security Agency-Ulusal Güvenlik Ajansı) tarafından analiz edildi ve bazı değişikliklerden sonra oluşturulan yeni algoritma, 1976'da NBS (National Bureau of Standards-Ulusal Standart Bürosu, daha sonra NIST olarak değişti) tarafından, DES (Data Encryption Standard- Veri Şifreleme Standardı) adıyla ABD'nin standart şifreleme algoritması olarak kabul edildi. DES 64 bit blok uzunluğunda, 56 bit anahtar boyu olan bir blok şifreleme algoritmasıdır.

DES'in standart olarak kabul edildiği yıl bir başka gelişme kriptolojide bambaşka bir ufuk açacaktı. Diffie ve Hellman IEEE'nin (Institute of Electrical and Electronics Engineers- Elektrik ve Elektronik Mühendisliği Enstitüsü) *Information Theory* (Bilgi Teorisi) dergisinde çıkan "Kriptografide Yeni Yönler" adlı makalelerinde, açık bir kanalda iki tarafın nasıl güvenli anahtar paylaşabileceğini anlatıyorlardı. Bu anahtar paylaşım protokolünün güvenliği matematikte ayrık logaritma probleminin çözümünün zorluğuna dayanıyordu. Böylece açık anahtarlı kriptografi doğmuş oldu. Hemen bir yıl sonra Rivest, Shamir ve Adelman açık literatürün ilk ve belki de en çok kullanılan açık anahtarlı şifreleme algoritmasını yayımladılar. Algoritmanın ismini kendi isimlerinin baş harflerinden oluşturmuşlardı: RSA. RSA'nın güvenliği de zor bir matematik problemine dayanır. Bu problem büyük sayıları çarpanlara ayırma problemidir.

1980'li ve 90'lı yıllarda kriptolojinin gelişimi ivme kazandı ve kriptoloji bir bilim olarak olgunlaştı. Sıradan insanların bilgi güvenliği ihtiyaçlarını karşılayan birçok uygulamanın bu yıllarda başladığını ve günümüzde de hızla yaygınlaştığını görüyoruz.

1980'li yılların sonlarında Koblitz ve Miller, şifrelemede ve sayısal imzalamada eliptik eğri üzerindeki ayrık logaritma probleminin kullanılabileceğini önerdiler. Eliptik eğri kriptosunda anahtar boyu diğer asimetrik kriptolarla karşılaştırıldığında son derece kısadır. Buna rağmen kripto camiası ilk yıllarda eliptik eğri kriptosunu şüpheyle karşıladı. Eliptik eğriler oldukça derin matematiksel objelerdi. Bu objeler üzerine kurulan kripto sistemlerin güvenliği hakkında hiç kimsenin tam bir fikri yoktu. Analizler zordu ve derin matematik bilgisi gerektiriyordu. Ancak yıllar ilerledikçe araştırmalar derinleşti. Yaklaşık yirmi yıllık yoğun kriptoanaliz çalışmalarına rağmen, şu ana kadar birkaç özel eliptik eğri dışında eliptik eğrilerin üzerindeki kriptonun zayıflığına dair bir sonuç bulunamadı. Dolayısıyla günümüzde eliptik eğri kriptosuna olan güven oldukça artmıştır.

1980'li yıllarda güvenli olduğuna inanılan DES, 90'lı yılların başında hızla itibar kaybetti. 1991'de Biham ve Shamir (RSA'nın S'si) tarafından yapılan diferansiyel atakla DES yara aldı. Atak pek pratik değildi ve uygulama için çok sayıda seçilmiş açık metin gerekiyordu. Asıl darbe iki yıl sonra Japonya'dan geldi. Mitsuri Matsui doğrusal kriptoanalizi keşfetti ve DES'in doğrusal atakla kırılabileceğini gösterdi. Hatta bir sene sonra pratik bir doğrusal atak düzenleyerek DES'i kırdı. Bu, literatürde DES'e uygulanmış ilk pratik ataktı.

Bütün bu gelişmeler artık DES'in şifreleme algoritması olarak ömrünü tamamladığını ve 2000'li yılların güvenlik ihtiyacını karşılamaktan uzak olduğunu gösteriyordu. NIST (National Institute of Standards and Technology-Ulusal Standartlar ve Teknoloji Enstitüsü) 1997'de yeni bir şifreleme standardı için yarışma başlattı. Yarışma 2001 yılında sonuçlandı. Rijmen ve Daemen adlı iki Belçikalı kriptoloğun tasarladığı Rijndael adlı algoritma AES (Advanced Encryption Standard- Gelişmiş Şifreleme Standardı) adıyla yeni standart şifreleme algoritması olarak seçildi. Günümüzde AES bütün dünyada en yaygın kullanılan şifreleme algoritmalarından biridir.

Kaynaklar

Kahn, D., *The Codebreakers: The Story of Secret Writing*, Scribner, 1996.
Menezes, A.J., Oorschot, P.C. ve Vanston, S.A., *Handbook of Applied Cryptography*, CRC, NY, 1997.
http://www.bletchleypark.org.uk
http://www.enigmahistory.org/

Orhun Kara

Dr., Başuzman Araştırmacı, UEKAE, TÜBİTAK

Kriptografinin Yapıtaşları

Kriptografik Algoritmalar ve Protokoller

Kripto sistemlerinin temellerini kripto algoritmaları ve bu algoritmaların hangi kurallarla kullanılacağını ifade eden kripto protokolleri oluşturur. Kriptolojinin varoluş nedeni olan gizlilik, kimlik doğrulama, inkâr edememe ve veri bütünlüğü gibi bilgi güvenliği hizmetleri, kripto algoritmaları ve protokolleri sayesinde sağlanır. Kriptografik algoritmalardan belki de en çok ilgi çekenler ve en yaygın kullanılanlar şifreleme algoritmalarıdır. İlginç olan ise günümüzde yaygın olarak kullanılan ve standartlaşmış modern şifreleme algoritmalarının hiçbirisiyle ilgili, kırılamayacağına dair henüz matematiksel bir ispat ortaya konamamış olması.

Anahtar Kavramlar

Simetrik şifrelemede, şifreleme yapacak ve çözecek kişiler arasında ortak bir anahtarda anlaşılmış olmalıdır.

Simetrik algoritmalarda şifreleme yapan aynı zamanda şifre de çözebilir. Oysa asimetrik algoritmalarda herkes şifreleme yapabilirken sadece özel anahtar sahibi şifreyi çözebilir.

Girdi olarak anahtar kullanmayan kripto algoritmaları da var. Örneğin, özet fonksiyonları rastgele uzunlukta metinleri girdi olarak alır ve sabit uzunlukta vektörler üretir. Bu vektörler metinlerin parmak izleri gibidir ve birçok kriptografik uygulamalarda uzun metinler yerine onları temsil ettiği düşünülen özetleri kullanılır.

Simetrik algoritmalar asimetriklere nazaran çok daha hızlıdır. Karşılaştırmak gerekirse simetrikler süpersonik uçaklar kadar hızlı ise asimetrikler ancak kağnı hızında olabilirler.

Kriptografik protokoller birçok açıdan resmi davet protokollerine benzer. Her ikisinde de davetli sayısı önemlidir. Kriptografik protokollerin çoğunda iki, üç, dört gibi az sayıda taraf (davetli) vardır.

Çoğu kriptografik sistemin öncelikli hedefi bilgiye yalnızca istenilen kişilerin ulaşabilmesini sağlamak, yani gizliliktir. Gizlilik, şifreleme (ve şifre çözme) algoritmalarıyla sağlanır. Şifreleme algoritması şifrelenecek metni ve şifreleme anahtarını girdi olarak alır. Şifrelenecek metne açık metin denir. Şifreleme algoritması bu iki veriyi kullanarak şifreli metni oluşturur. Şifre çözme algoritmasındaysa şifreli metin ve şifre çözme anahtarı kullanılarak açık metin üretilir. Şifre çözme algoritmasını şifreleme algoritmasının ters fonksiyonu gibi düşünebiliriz. Şifreyi nasıl çözeceğimizi bilmeden şifrelemeyi bilmek işimize yaramayacağı için kriptologlar çoğunlukla ikisine birden "şifreleme algoritması" derler.


JUPITERIMAGES

Şifreleme algoritmaları denilince önce hem şifreleme işleminde hem de şifre çözme işleminde aynı anahtarın kullanıldığı simetrik şifreleme algoritmaları akla gelir. Simetrik şifrelemede kullanılan anahtar başkalarından gizli tutulduğu için bu anahtara gizli anahtar denir. Bu yüzden simetrik şifrelemenin bir diğer adı da gizli anahtarla şifrelemedir.

Simetrik şifrelemede, şifreleme yapacak ve çözecek kişiler arasında ortak bir anahtarda anlaşılmış olmalıdır. Bunu sağlamanın bir yolu anahtarı, şifreleyecek ve şifre çözecek kişilere güvenli bir kanaldan ulaştırmaktır. Burada aklınıza şu soru takılabilir. Anahtarı güvenli bir kanaldan ulaştırıyorsak mesajı neden doğrudan o kanaldan göndermeyelim? Öncelikle, algoritmanız yeterince güçlüyse



Kriptografi sayesinde internette kredi kartı numarası, vatandaşlık numarası gibi hassas bilgilerimizi yetkili kişilere güvenle iletebilir, güvenli alışveriş yapabilir, bankacılık işlemleri gerçekleştirebilir, faturalarımızı ödeyebilir, belge imzalayabiliriz.

ve anahtarınız yeterince güvenli saklanıyorsa şifreleme anahtarını milyarlarca defa kullanabilirsiniz! Sonra anahtarlar mesajlara göre çoğunlukla çok kısa boydadır. Örneğin, 128 bit ya da 256 bit. Bu anahtarla gigabaytlarca veri şifreleyebilirsiniz. Ayrıca güvenli kanal her zaman açık olmayabilir.

60 farklı internet kullanıcısının birbirleriyle simetrik şifrelemeyle haberleşmek istediklerini varsayalım. 60 kullanıcının 60'ı da aynı anahtarı paylaşıyor, yani tek bir anahtarla yetiniyor olabilir. Bu durumda hepsi diğerlerine gelen/giden mesajları okuyabilir. Diyelim ki bu kişiler birbirlerinden gizlisi saklısı olmayan insanlar. Dolayısıyla bu durumdan rahatsız değiller. Fakat içlerinden birisi çok dikkatsiz ve bu anahtarı koruyamamış. Bu durumda tek bir dikkatsiz kullanıcı yüzünden 60'ının da mesajları okunuyor olacak. O zaman bütün kullanıcı çiftleri ayrı bir anahtar paylaşsın. Bakalım ne kadar anahtara ihtiyaçları var? Hesaplayalım: 60×59/2, yani 1770 farklı anahtar!

Peki ya bin kişi birbirleri ile haberleşecekse? Ya biri yüzünden bini de anahtarını kaptıracak ya da yüz binlerce anahtar dağıtılacak. Kırk katır mı, kırk satır mı? İşte bu sorun asimetrik şifreleme algoritmaları sayesinde aşılabilir. Asimetrik şifreleme algoritmalarına sonra tekrar değinmek üzere, şimdi simetrik şifreleme algoritmalarını incelemeye devam edelim.

Simetrik şifreleme algoritmalarını iki grupta incelemek mümkün: Blok şifrele-

Gizli Anahtara Karşı Açık Anahtar

Gizli anahtarla şifrelemenin (simetrik şifreleme) binlerce yıllık geçmişe sahip olmasına karşın, açık anahtarlı şifreleme (asimetrik şifreleme) henüz 32 yaşında! Açık anahtar kriptografisi Diffie ve Hellman'ın 1976'da buldukları anahtar paylaşım protokolüyle doğmuş oldu. Bir sene sonra Rivest, Shamir ve Adleman tarafından tasarlanan tarihin ilk açık anahtarlı şifreleme algoritması RSA yayınlandı.

Peki ama biz şifreleme yapacaksak ne tür bir algoritma kullanacağız? Açık anahtarlı mı, gizli anahtarlı mı? Her iki türün de kendine göre avantajlı olduğu yerler var.

Simetrik şifreleme hem donanımda hem de yazılımda çok daha hızlıdır. Aralarındaki hız farkını gözünüzde canlandırmak istiyorsanız bir kaplumbağa ile bir jetin hızını düşünün! Sabit diskinizi asimetrik bir algoritma ile şifrelemeye karar verdiyseniz bir kez daha düşünmelisiniz!

Simetrik olanların gerçeklenmeleri de çok daha kolay. Genellikle simetrik algoritmalarda elektronik yongaların sevdiği ve/veya, dışarlayıcı-veya (XOR) gibi basit işlemler kullanılırken, asimetrik algoritmalarda devasal kümelerde çarpma, üs alma, bölme, ters alma gibi yongaları ve işlemcileri zorlayan aritmetikler kullanılır. Üstelik genel olarak asimetrik olanların anahtar boyları çok daha uzundur. Örneğin 80 bitlik bir simetrik algoritmanın sağladığı güvenliği 1024 bitlik bir RSA sağlayabilmektedir. Kütüphanelerdeki kitapların kapaklarına yapıştırılmış RFID etiketlerinde dahi bir simetrik algoritma koşturabilirsiniz. Oysa bir asimetrik algoritmayı gerçeklemek için pahalı ve büyük bir yongaya ihtiyacınız var.

Simetrik sistemler sayesinde hızlı bir şekilde veri bütünlüğü sağlamak da mümkün.

Buraya kadar hep simetrik algoritmaları övdük; sıra asimetrik algoritmalarda! Kullanıcı sayısının çok olduğu bir uygulamada anahtar paylaşımı ve tutulması gereken anahtar sayısı açısından asimetrik algoritmalar oldukça başarılıdırlar.

Kullanıcılardan herhangi ikisinin kendi aralarında, diğerlerinin dinleyemeyeceği kriptolu haberleşmeleri gereksin. Simetrik şifreleme ile kullanıcı sayısının ikili kombinasyonu kadar anahtar çiftinin kullanıcılar arasında güvenli kanallardan paylaştırılması gerekmektedir. Oysa asimetrik sistemde herhangi iki kullanıcı kullanıcı sayısı kadar anahtar çiftiyle kendi aralarında kriptolu haberleşebilir. Aslında simetrik algoritmaların en büyük eksikliği ve asimetrik olanların da ortaya çıkış nedeni bu problemdir.

Asimetrik şifrelemede çok az sayıda anahtarla problemi çözebiliriz. Üstelik güvenli kanaldan gizli anahtar paylaşımına da gerek yok. Çünkü gizli kalması gereken anahtarlar zaten paylaşılmıyor. Yalnızca açık anahtarlar paylaşılıyor, onlar da gizli olmak zorunda değiller. Açık anahtarlı sistemlerdeki bir sorun, açık anahtarın gerçekten sahibine ait olup olmadığını göstermektir. Saldırgan kendi açık anahtarını sizin açık anahtarınız gibi kabul ettirirse, sizin adınıza işlemler yapabilir. Bu nedenle açık anahtarlar genellikle güvenli biri tarafından sertifikalandırılarak dağıtılır.

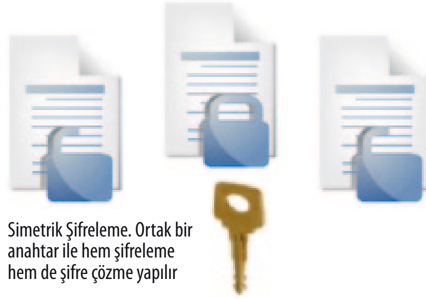
Asimetrik sistemlerden vazgeçemememizin bir nedeni de, inkâr edememe hizmetinin ancak asimetrik sayısal imza algoritmalarıyla sağlanabilmesi. Asimetrik şifrelemede olduğu gibi, burada da "özel" işlem, yani imzalama işlemi özel anahtarla, herkesin yapabileceği işlem, yani imza doğrulama işlemi açık anahtarla yapılır. Nasıl ki, asimetrik şifrelemede de herkes şifreleme yaparken sadece özel anahtar sahibi şifre çözebiliyorsa, imzayı sadece yetkili atabilirken, herkes doğrulayabiliyor.

Görünen o ki her iki şifreleme türü de farklı alanlarda birbirlerine üstünlük kurmuşlar. Bu nedenle kriptologlar hibrit (melez) sistemler tasarlamayı tercih ederler. Anahtar şifreleme, anahtar anlaşma ve sayısal imza işlemleri genellikle asimetriklerle, yığın veri şifrelemeleri ve imzasız veri bütünlüğü korumaysa simetriklerle gerçekleştirilir.

me algoritmaları ve dizi şifreleme algoritmaları. Blok şifreleme algoritmaları metinleri uzunlukları belli olan bloklar halinde şifreler. Dolayısıyla her bir anahtar belli blok uzunluğunda bir permütasyon belirler. Bu permütasyonlar bir açık metin bloğuna karşılık hangi kapalı metin bloğu çıkacağını ifade eder. Blok şifreleme algoritmalarında içsel bir hafıza yoktur. Dolayısıyla şifreleme zamana bağlı değildir. Bu yüzden blok şifreleme algoritmalarına hafızasız şifreleme de denir. Veri Şifreleme Standardı (DES), Gelişmiş Şifreleme Standardı (AES) ve Uluslararası Şifreleme Algoritması (IDEA) gibi şifreleme algoritmaları birer blok şifreleme algoritmasıdır.

Dizi şifreleme algoritmalarında bir üreteç aracılığıyla, anahtar yardımıyla istenildiği kadar uzun bir dizi üretilir. Bu diziye, kayan anahtar denir. Kayan anahtar üretimi genellikle karmaşık fonksiyonlarla yapılır. Kayan anahtarla açık metnin "toplanmasında" basit matematiksel işlemler kullanılır. Kayan anahtar üretimi sırasında, üreteç içerisinde bir içsel durum vektörü oluşturulur. İçsel durum vektörü zamana bağlı olarak güncellenir ve kayan anahtar üretiminde kullanılır. Dolayısıyla kayan anahtar zamana bağlıdır ve hafızadaki durum vektörü şifrelemede rol oynar. Bu yüzden dizi şifreleme algoritmalarına hafızalı şifreleme de denir.

Dizi şifreleme algoritmalarının en ilginç özelliği kayan anahtar üretimi sırasında açık metnin girdi olarak kullanılmaması ve asıl karıştırıcı fonksiyon olan kayan anahtar üretecine açık metnin girmemesidir. Açık metin şifrelemenin en son adımında şifreleme işlemine basit bir metamatiksel işlemle dâhil edilir. Dolayısıyla şifreli metinde açık metnin karıştırım (confusion) ve yayınımını (diffusion) göremeyiz. Diğer bir deyişle, açık metindeki değişiklikler şifreli metne aynen yansır. Bunun tersi de doğrudur. Şifreli metindeki değişiklikler açık metinde ancak karşılık gelen karakterleri etkiler. Böylece şifreli metin karşı tarafa iletilirken ortamdaki gürültüden kaynaklanan hatalar yayılmaz.



Simetrik Şifreleme. Ortak bir anahtar ile hem şifreleme hem de şifre çözme yapılır

Hatanın yayılmaması nedeniyle yüksek frekanslı telsiz haberleşmelerinde olduğu gibi gürültülü ortamlardaki ses iletimini şifrelemek için genellikle dizi şifreleme kullanılır. Hatanın yayılmaması sayesinde ses, ortamdaki gürültüye rağmen alıcı tarafından anlaşılabilir. Diğer taraftan, hatanın yayılmaması açık metindeki bütünlük kontrolünü zorlaştırır. Dolayısıyla bütünlüğün önemli olduğu haberleşmelerde genellikle dizi şifreleme yerine blok şifreleme algoritmaları tercih edilir.

Minik Diziler Mini Minnacık Bloklar

Yaklaşık son beş yıla kadar dizi şifreleme algoritmalarının blok şifreleme algoritmalarına kıyasla daha basit olduğu,

Uğur Kaşif Boyacı

Uzman Araştırmacı,
UEKAE, TÜBİTAK

Kriptonun Olmazsa Olmazı Anahtar

Pahalı ve güvenli bir arabanız var. Arabanızın motor kilidi "immobilizer", anahtarınız olmadan arabanızın çalışmasını olanaksız hale getiriyor. Böylece arabanıza düz kontak dahi yapılamıyor. Arabanızın kapıları da anahtarsız mümkün değil açılmıyor. Camlar kırıldığında ya da kapılar zorlandığında alarm devreye giriyor. Hırsızların hiç şansı yok! Arabanız gerçekten de güvende. Ama bir dakika! Eğer anahtarınız güvende ise! Anahtarınızı kaybederseniz ya da çaldırırsanız araba hırsızları arabanıza sizin kadar yakın demektir. Modern kripto sistemlerinde de güvenlik anahtarın güvenliğine indirgenmiştir. Dolayısıyla anahtarlar kripto sistemlerinin yumuşak karnıdır. Bu nedenle bir anahtarın bütün varoluş süreçleri boyunca özenle korunması şart.

Kripto sistemlerinin kalbi anahtarlardır, bu nedenle anahtarlarımızı gözümüz gibi korumalıyız. Daha teknik bir ifade ile "bir kripto sisteminin güvenliği anahtarların gizliliğine dayanmalıdır". Bu ilke 19. yüzyılda yaşamış Fransız dilbilimci Auguste Kerckhoff tarafından ortaya atılmıştır. Sisteminiz, şifreleme algoritmanız ve yaptığınız her türlü matematiksel işlem ve fonksiyonlar bir şekilde düşmanın eline geçebilir. Bu durumda dahi sisteminiz güvenli olmalı. Güvenliğinizi algoritmanın ya da haberleşme protokolünün gizli olmasına, açık metinlerin tahmin edilemez ve karmaşık olmasına dayandırırsanız ciddi bir risk altındasınız demektir.

Kerckhoff ilkesinin ilginç bir özelliği de dünyada en çok yanlış algılanan ilkelerden biri olmasıdır. İlkeyi yanlış algılayanlar, genellikle algoritmanızı ve protokolünüzü en ince detayına kadar açıklamanız gerektiğini ve sadece anahtarınızın gizli kalması gerektiğini ifade ederler. Oysa Kerckhoff'un anlatmak istediği il-

donanımda daha az yer kapladığı kanısı hâkimdi. Blok şifreleme algoritmalarının da yazılımda, özellikle masaüstü işlemcilerinde çok daha hızlı olduğu düşünülüyordu. Son yıllarda yapılan araştırmalar ve geliştirilen yeni şifreleme algoritmaları bu ezberi bozacak gibi görünüyor.

Avrupa Birliği 6. Çerçeve Programı Mükemmeliyet Ağları projesi kapsamında 2004'de başlayıp geçen yıl sona eren Estream Projesi dizi şifreleme algoritması tasarımı ve analizi üzerine odaklanmıştı. Projenin bir ayağında özellikle donanımda çok az yer kaplayan, yani olabildiğince az sayıda devre kapısıyla gerçeklenen dizi şifreleme algoritmaları masaya yatırıldı. Bu kategoride en çok ilgi çeken iki algoritma Trivium ve Grain oldu. Wili Meier ve arkadaşları tarafından tasarlanan Grain, yaklaşık 1500 devre kapısıyla, Christophe De Canniere ve Bart Preneel tarafından tasarlanan Trivium ise 2500-3000 devre kapısıyla gerçeklenebilmektedir. Donanımda hız öncelikli bir AES gerçeklenmesinin yaklaşık 100.000 devre kapısı kadar yer kapladığı düşünülürse her iki dizi şifreleme algoritmasının da donanımda ne kadar az yer kapladığı daha iyi anlaşılır.

Grain de Trivium da dizi şifreleme algoritmalarının donanımda ne kadar az yer kaplayabileceğine iyi birer örnek olsa da, bu algoritmalardan birkaç yıl sonra tasarlanan bir blok şifreleme algoritması az yer kaplama açısından dizi şifreleme algoritmalarının tahtını salladı diyebiliriz. Aralarında Lars Knudsen ve Matt Robshaw gibi kriptologların bulunduğu bir grup tarafından tasarlanan ve yaklaşık 1500 devre kapılık yer kaplayan PRESENT adlı blok şifreleme algoritması 2007'de CHES (Cryptographic Hardware and Embedded Systems-Kriptografik Donanım ve Yerleşik Sistemler) konferansında yayınlandı. Geçtiğimiz aylarda Orr Dunkelman ve Christophe De Canniere tarafından tasarlanan KATAN adlı bir blok şifreleme algoritmasının bir sürümüyse sadece 500 devre kapılık yer kaplıyor! Tasarımcılardan alınan bilgiye göre algoritmanın bu yılın ikinci yarısında bir kriptoloji konferansında yayınlanması planlanıyor. Kriptolojideki bu son gelişmeler donanımda dünyanın en küçük algoritmalarının artık dizi şifreleme algoritmaları yerine blok şifreleme algoritmaları olduğunu göstermektedir. Ama yarış devam ediyor. Kim bilir, belki gelecekte dizi şifreleme algoritmaları tahta tekrar oturur.

Masaüstü Bilgisayarlarda Kim Önde?

Son on yıla kadar, kriptologlar arasında blok şifreleme algoritmalarının masaüstü işlemcilerde dizi şifreleme algoritmalarına kıyasla çok daha hızlı ve verimli çalışacağı kanısı hâkimdi. Kriptologlar aslında böyle bir kanıya varmakta haksız da değiller. Modern masaüstü işlemciler 32 bit ya da 64 bit gibi kelimeler üzerinde işlemler yaparlar ve blok halinde işlemleri başarıyla gerçeklerler. Diğer taraftan bu işlemcilerdeki seri işlem mantığı, yazmaç tabanlı dizi şifreleme algoritmalarında hafızaların güncellenmesi türünden işlemlerin hızlı gerçeklenmesine çok uygun değildir. Gerçekten de 70'li ve 80'li yılların donanıma özel tasarlanmış dizi

ke şöyledir: Kripto sisteminiz öyle bir özelliğe sahip olacak ki, bütün sistem detayları açığa çıksa dahi anahtar gizli kaldığı sürece sisteminiz (kriptografik açıdan) güvenli olacak. Tarihte yaşanmış tecrübelerle Kerckhoff ilkesini benimsemenin ne kadar önemli olduğu defalarca kanıtlanmıştır.

Algoritmanız öyle tasarlanmış olmalı ki, biri nasıl çalıştığını bilse bile anahtarı bulmadan ondan yararlanamamalı. Hatta saldırganın elinde "bol miktarda" algoritma girdisi ve çıktısı bulunsa dahi anahtar hakkında bilgi edinememeli. Bol miktarda derken aynı kategorideki ideal bir algoritmanın karmaşıklığı kastedilmektedir. Örneğin bir simetrik şifreleme algoritması için bu anahtar uzayının neredeyse tamamı demektir. Tabii böyle matematiksel fonksiyonlar tasarlamak tam bir uzmanlık alanı.

Diyelim ki şifreleme algoritmanız sağlam ve saldırgan algoritmayı analiz yoluyla kıramayacağını anladı. O zaman doğrudan anahtarın kendisini hedef alır. Eğer anahtarı daha kolay elde edebilecekse neden yıllarca matematiksel denklemler kurarak, binlerce bilgisayara iş vererek sonuç beklesin ki?

Saldırgan anahtarı "doğumunda", "ölümünde" hatta "mezarda dahi" ele geçirirse yine de avantaj elde edebilir. Evet, anahtarların bir yaşam döngüsü vardır! Anahtarlar sipariş edilir, üretilir, paketlenir, adreslerine teslim edilir, saklanır, kullanılır, işleri bitince de atılır ve gerekirse yok edilir, yerine yenileri gelir. İşte bu yaşam döngüsü boyunca anahtarlara nasıl bakılacağına "anahtar yönetimi" denir.


Visual Photos

Bir anahtarın yaşam döngüsünün ortasına bakalım; yani anahtar saklamaya... Neden ortasından başlıyoruz? Anahtarın saklanması her kullanıcının derdi de ondan. Kişisel bilgisayarımızda anahtarları nasıl saklayabiliriz? Akla ilk gelen cevaplar ya "güvenli bir yerde" ya da "şifreleyerek". Peki bilgisayarınızın güvenli yeri neresi? Günümüzde bilgisayarların sabit diskini sökerek içinden bilgi okunması çok zor değil. Ayrıca internete bağlıysanız saldırgan bilgisayarınıza uzaktan da erişebilir. Peki o zaman bütün anahtarlarımızı başka bir anahtarla şifreleyelim. Bu sefer de anahtar şifreleme anahtarı için aynı soru geçerli. Anahtar şifreleme anahtarını nasıl saklayacağız? Eninde sonunda bir anahtarı güvenli bir şekilde saklamamız gerekir.

Bir kripto sisteminde bütün anahtarlar aynı kıymette olmayabilir. Yukarıdaki çözümde anahtar şifreleme anahtarı diğer anahtarlardan daha kıymetlidir, çünkü anahtar şifreleme anahtarı ele geçirilirse diğerleri de ele geçirilmiş olur. Kıymetli anahtarlarımızı taşınabilir bir

şifreleme algoritmaları masaüstü işlemcilerde bir kağnı kadar yavaştı.

Kriptoloji gibi baş döndürücü bir hızla gelişen bir bilimde, masaüstü işlemcilere uygun ve güvenli birçok dizi şifreleme algoritmasının tasarlanması hiç de şaşırtıcı değil. Hatta öyle dizi şifreleme algoritmaları vardır ki masaüstü işlemcilerde bilindik tüm blok şifreleme algoritmalarından daha hızlı olduklarını söyleyebiliriz. Örneğin Hongjun Wu tarafından tasarlanıp 2004'de Estream projesine sunulan ve şu ana kadar henüz bir zayıflığı keşfedilemeyen HC-128 adlı dizi şifreleme algoritması masaüstünde yaklaşık 2 devirde bir bayt üretebiliyor. Örneğin 2 GHz frekansı olan bir işlemcide saniyede 1 GB (gigabayt) veriyi şifreleyebiliyor. Bu, AES'in yazılımda en hızlı gerçeklenmesinden yaklaşık 6 kat daha hızlı. Tabii, Intel'in bu sene sonunda piyasaya süreceği, içinde AES şifreleme ve şifre çözme komut takımının bulunacağı işlemcileri dikkate almazsak... Bu yeni nesil işlemcide AES çok daha aşağı katmanda, donanımda Intel mühendislerinin özel olarak tasarladığı ve gerçeklediği yonga üzerinde koşuyor olacak. Test sonuçları şimdiden etkileyici: Bu işlemciler sayesinde, AES en az üç kat daha hızlanacak. Ama donanımdan gelen bu ayrıcalığa rağmen AES yine de HC-128 kadar hızlı olamayacak!

Yeri gelmişken HC-128'in güvenliği hakkında bir not ekleyelim. Ünlü Hint kriptolog Maitra öğrencileriyle birlikte yaptığı altı aydan uzun süren yoğun bir çalışma sonucunda HC-128'in iç yapısıyla ilgili "beklenmedik" bazı özellikler keşfetti. Çalışmanın sonuçlarını geçen Mayıs ayında Norveç'te düzenlenen Uluslararası Kodlama Teorisi ve Kriptografi Çalıştayı'nda (WCC) anlattılar. Sunumlarını "Biz algoritmada henüz bir zayıflık keşfedemedik. Ama belki başkaları bizim keşfettiğimiz sapmaları daha da geliştirip HC-128'i kırmayı başarabilir," diyerek sonlandırdılar.

Anahtarsız Algoritmalar

Girdi olarak anahtar kullanmayan kripto algoritmaları da var. Bunlar genellikle tek başlarına bir hedefe ulaştırmıyor fakat sistem içinde diğer algoritmalara çok yardımcı oluyorlar. Anahtarsız algoritmalardan en bilineni özet fonksiyonlarıdır (hash functions). Bu algoritmaların kullanım alanlarında sağlamaları gereken özelliklerle ilgili olarak kendilerine özgü güvenlik ölçütleri bulunur.

Özet fonksiyonları girdi olarak rastgele uzunlukta metinleri alır, sabit uzunlukta (genellikle 20-64 bayt arası) vektörler üretir, bir nevi metinlerin parmak izlerini alır ve birçok kriptografik uygulamada uzun metinler yerine onları temsil ettiği düşünülen özetleri kullanılır.

Özet fonksiyonları bütünlük denetiminde ve güvenli parola saklamada yaygın olarak kullanılır. Güvenlik nedeniyle bilgisayarlarda parolalarımızın kendileri saklanmaz. Bunun yerine, parolalarımızın "tuz" denilen, rastgele üretilmiş vektörlerle birlikte özetleri alınır ve bunlar saklanır. Bu yüzden özet fonksiyonları tek yönlü fonksiyonlar olmalıdır, yoksa diğer yönden parolayı elde ederiz. Yani bir metnin özetini almak hesapsal olarak kolayken, verilmiş bir özete sahip bir metin oluşturmak pratikte mümkün olmayacak kadar zor olmalıdır. Bu özelliğe,

cihazda saklayabiliriz. Böylece hem anahtarları başka yerde de kullanabiliriz, hem de anahtarlar "gözümüzün önünde" olur. Özellikle anahtar saklamak üzere üretilmiş taşınabilir cihazlar vardır. Bu cihazlarda anahtarlar şifreli olarak saklanır. Saldırganın erişemeyeceği, erişmeye çalıştığı takdirde silinen küçük bir bellekte ise bu anahtarları şifreleyen anahtar saklanır. Bu anahtar da genellikle parola ile korunur. Böylece anahtar saklayan mini cihaz ele geçse bile anahtarlarımıza parola bilinmeden ulaşılamaz.

Anahtar saklamanın bir diğer yolu da anahtarı ikiye ayırmaktır! Bir parçasını bilgisayarınızda, diğer parçasını ise taşınabilir fakat çok da güvenli olmayan bir ortamda, örneğin bir bellek kartında saklarsınız. Karttan okunan parça ile bilgisayardaki parça bir araya gelince anahtar geri kazanılır. Bir saldırganın parçalardan birini öğrenmiş olma ihtimaline karşı birkaç kullanımdan sonra farklı bir parçalama yapılarak anahtar farklı bir şekilde ayrılır. Böylece saldırgan elini çabuk tutmazsa öğrendiği parça işine yaramaz.

Gelelim anahtarların doğumuna! Eğer anahtar üretimi sonucunda tahmin edilebilir anahtarlar çıkıyorsa saldırgan da bunları tahmin edebilir. Bu nedenle anahtarlar mümkün olduğunca rastsal üretilmelidir.

Meşhur bilgisayar bilimci Donald Knuth'un söylediği gibi "Rastsal sayılar rastgele metotlarla üretilmemelidir." Tam aksine rastsal sayı üreten mekanizmaların tasarımı ve gerçekleştirilmesi büyük özen ister.

Rastsal sayı üreteçleri temel olarak ikiye ayrılır. Bir diyotun anlık elektrik akımı ya da kaotik bir sistem gibi fiziksel olaylara dayalı olarak rastsal sayı üreten mekanizmalara "Gerçek Rastsal Sayı Üreteci" (GRSÜ), matematiksel yollardan çekirdek bir değerden deterministik olarak rastsal sayı dizileri üreten mekanizmalara "Sanki Rastgele Sayı Üreteci" (SRSÜ) denir.

Her ne kadar adı "gerçek" ile başlasa da gerçek rastsal sayı üretecilerin gerçekten rastsal sayı ürettiğinden emin olmak kolay değildir. Aşırı ısı, elektrik yüklemesi, manyetik alan gibi dış etkenlerden dolayı gerçek rastsal sayı üreteci çıktıları tahmin edilebilir dizilere dönüşebilir.

Buna karşılık sanki rastgele sayı üreteci çekirdek bilinirse üretilen rastsal değerlerin hepsi ortaya çıkar. Bu nedenle çekirdek saldırgan tarafından tahmin edilememelidir. Ayrıca saldırgan sanki rastgele sayı üreteciyi aynı çekirdeği yutmaya ikna ederse sanki rastgele sayı üretecilerde aynı dizi ortaya çıkar. Bazı algoritma ve protokollerde anahtar kadar önemli, taze oluşturulmuş değerler gereklidir.

İstatistiksel Testler

Bir üretecin rastsal sayı ürettiğinden emin olabilir miyiz? Rastsallık konusuyla uğraşan matematikçi ve istatistikçiler "Hiçbir test tek başına rastgeleliğe karar veremez" demektedir. Çeşitli istatistiksel ve matematiksel testlerle üreteç çıktısından topladığımız numune dizilerinin beklediğimiz belli "davranış profilleri"ne uyup uymadığını kontrol ederiz. Davranış profilleri genelde

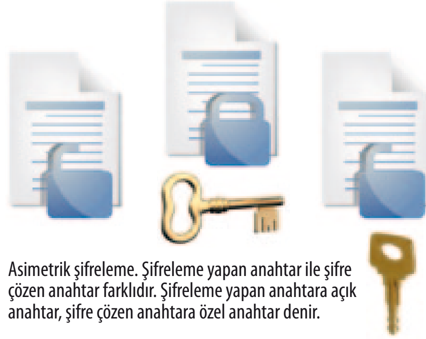
ters-görüntüye dayanıklılık deniyor. Böylece bir parolanın özet değerini ele geçirseniz bile, parolayı ortaya çıkaramazsınız.

Özet fonksiyonlarının kullanıldığı bir başka uygulama ise sayısal imza algoritmalarıdır. Asimetrik algoritmalar kullanıldığı için imza algoritmaları oldukça yavaştır. Dolayısıyla büyük metinlere doğrudan imza atmak uzun zaman alır. Üstelik imza da metin kadar büyük olursa, imzalı metin kaynak metnin iki katı yer kaplayacaktır. Bu nedenle önce metnin özeti alınır, sonra özete imza atılır. Özet almak imza atmaya kıyasla çok daha hızlı bir işlem olduğundan, uzun verilere imza atmak kısa verilere imza atmak kadar hızlı olacaktır. Ancak burada dikkat edilmesi gereken bir güvenlik problemi var. Performanstaki bu kazanım güvenlik açığına neden olmamalı! Herhangi iki metin aynı özeti veriyorsa birine atılan imza diğeri için de geçerli olacaktır. Dolayısıyla bir metinle aynı özeti üretecek ikinci bir metin bulmak hesapsal olarak zor olmalı. Özet fonksiyonların bu güvenlik ölçütüne ikinci ters-görüntüye dayanıklılık denir.

Asimetrik Şifreleme

Asimetrik şifrelemede şifreleme anahtarı ile şifre çözme anahtarı farklıdır. Şifreleme yapan anahtara açık anahtar, şifreyi çözen anahtara özel anahtar denir. Açık anahtar adından da anlaşılacağı gibi açıktadır, dost düşman herkese verilebilir! Herhangi birine gizli mesaj göndermek isteyen, o kişinin açık anahtarı ile açık metni şifreler. Şifreyi çözebilecek olan kişi yalnızca özel anahtarın sahibidir. Özel anahtar kişiye özeldir ve kimseyle paylaşılmaz.

Simetrik şifreleme ile asimetrik şifreleme kavramları arasındaki temel farkı daha açık anlatabilmek için kapı kilitleri ile asma kilitli posta kutusunu örnek verebiliriz. Evimizin dış kapısını kilitlemek ya da açmak için kullandığımız anahtarların simetrik şifrelemede gizli anahtara karşılık geldiğini düşünebiliriz. Bu anahtarlar ile hem kapıyı kilitleyebilir (şifreleme yapabilir) hem de kilitli kapıyı açabiliriz (şifreyi çözebiliriz). Herkesin ulaşabileceği, asma kilitli bir posta kutusunu açık anahtar olarak düşünün. Posta kutusuna herkes mesaj atabilir, ama posta kutusundaki mesajları yalnızca kutuyu açan asma kilit anahtarına sahip olan okuyabilir.



Asimetrik şifreleme. Şifreleme yapan anahtar ile şifre çözen anahtar farklıdır. Şifreleme yapan anahtara açık anahtar, şifre çözen anahtara özel anahtar denir.

KRİPTO PROTOKOLLERİ

Protokol denilince çoğumuzun aklına milli bayramlardaki resmigeçit törenleri ya da smokin veya frak giymiş devlet adamlarının bulunduğu resmi davetler gelir. Resmi davetlerde, kimin kiminle nasıl selamlaşacağı, kimin hangi sırada salona gireceği, yemekte kimin yanına kimin oturacağı sıkı kurallara bağlanmıştır. Protokol belli amaç ve hedefler için, belli bir ortamda, taraflar arasında sırasıyla uyulması gereken iş adımlarını ifade eder.

miktar, büyüklük, sıralanma ya da tekrar etme üzerine kuruludur. Üreteç çıktısı belli profillere uysa da sayıların rastsallığından emin olamayız, ancak şüphelerimizi azaltabiliriz.

İstatistiksel testlerden geçemeyen bir üreteç çok büyük bir ihtimalle kötü tasarlanmıştır. Emin olduğumuz şey: Eğer üreteç istatistiksel testlerden kalıyorsa üreteçte defo vardır! Diğer yandan kötü olduğunu bildiğimiz, yani üreteceği diziyi tahmin edebildiğimiz fakat yapılan istatistiksel testlerden başarıyla geçen üreteçler de vardır. Bu nedenle rastsallıktan uzak üreteçleri yakalamak için istatistikçiler yeni ve pratik testler aramaya devam etmektedir.

Anahtar Üretim/Dağıtım Merkezi

Rastsal sayı üretecinden elde edilen çıktılar, her kriptografik algoritma için anahtar olarak kullanılmaya elverişli değildir. Bazı şifreleme algoritmalarında zayıf, yani saldırganın algoritma girdi-çıktılarından kolayca tahmin edebileceği anahtarlar vardır. Üretilen anahtarın zayıf olup olmadığının kontrol edilmesi gerekir.

Anahtarları gerekli rastsallıkta ve doğru ölçütler altında üretmek, gerekli kişilerce paylaşımını sağlamak, anahtar üretim maliyetini düşürmek ve benzeri nedenlerle, en azından bazı kritik anahtarlar herkes tarafından güvenilen bir anahtar üretim merkezinde üretilmektedir.

Anahtarların doğru adrese teslimini, gittikleri yerde doğru zamanda ve doğru amaçla kullanılmasını sağlamak için anahtarlar etiketlenir. Etiketleme yanlış yapılırsa anahtarlar yanlış kişilerin eline geçebilir ya da kullanıcıya ulaştırılamaz. Etiket üzerinde anahtarın son kullanım tarihi gibi bilgiler de bulunur. Dağıtım sırasında başına bir şey gelmemesi ve kolay taşınması için anahtarlar paketlenmelidir.Genellikle paketin hem içinde, hem dışında birer etiket bulunur.



Saldırgan anahtarı dağıtım sırasında ele geçirmeye de kalkabilir. Eğer anahtar kurye ile elden taşınıyorsa, saldırgan anahtarı ele geçirmek için anahtarı taşıyan kuryeye zarar vermeyi bile göze alabilir ya da kuryeyi kandırmaya kalkabilir. Saldırgan kuryeden elde edeceği anahtarın şifreli olduğunu ve açamayacağını bir şekilde bilirse kurye büyük bir ihtimalle hedef olmayacaktır.

Bir Anahtar Taşıma ve Yükleme Cihazı: KAYC-S

Anahtar üretim merkezinden cihaza güvenli taşımanın emin bir yolu, merkezin paketi güvenli hattan (saldırganın kolayca mü-

Kriptografik protokoller birçok açıdan resmi davet protokollerine benzer. Her ikisinde de davetli sayısı önemlidir. Kriptografik protokollerin çoğunda iki, üç, dört gibi az sayıda taraf (davetli) vardır. Bazı protokollere ise çok sayıda taraf katılır. Hizmet kalitesini düşürmeden ve maliyeti aşırı yükseltmeden kriptografik protokolü işletmeye ölçeklenebilirlik denir. Ölçeklenebilirlik iyi bir “çok taraflı protokol”ün en aranan özelliklerinden biridir.

Resmi davetlerde çoğu zaman davetlilerin katılımını sağlayacak bir davetiye vardır. Protokollere tarafların katılımı kriptografik anahtarlar sayesinde olur. Anahtar ve “davetiye” arasında önemli bir fark vardır. Davetliler davetiyelerini başkalarına gösterebilirler fakat kriptografik protokollerde anahtarları, paylaşanlar dışında kimse görmemelidir. Neden mi? Elektronik ortamda davetsizlerin anahtarı kopyalaması çok kolaydır da ondan. Bazı davetlerde özenle saklanması gereken eşyalar bulunur. Örneğin bir kraliçenin takısı paha biçilemez olabilir. Kriptografik protokollerde de bazı anahtarlar saldırganlar için mücevherlerden daha değerlidir.

Nasıl davetlerin kapalı mekân, maskeli balo ya da resmigeçit töreni olması kuralları değiştirebiliyorsa, kriptografik protokollerde de ortam belirleyici olur. Örneğin kullanılan hattın telsiz, telefon, cep telefonu, kablolu internet, uydu haberleşmesi olması ve bu hatların gürültü oranı gibi karakteristikleri, protokol tasarımını derinden etkileyebilir.

Davetlilerin niteliği de protokolü değiştirir. Örneğin bazı protokollerde mutlaka herkesin güvendiği biri gerekir. Biz bu davetliye “Güven” diyelim. Güven genellikle bir anahtar dağıtım merkezi ya da sertifika otoritesidir. Bazı protokollerde davetlilerin bir kısmı işlemleri kolayca ve hızlıca yapabilirken bir kısmının eli yavaştır. Örneğin RFID protokollerinde okuyucular hızlı işlem yaparken RFID etiketleri kısıtlıdır. Bazı protokollerdeyse başı çok kalabalık davetliler olacağını hesaba katmak gerekir; örneğin istemci-sunucu protokolleri...

Kriptografik protokolleri asıl ilginç kılan, protokollere katılan davetsiz ya da münasebetsiz katılımcılardır. Davetsizlere saldırgan diyeceğiz. Davetli listesinde olduğu halde protokol kurallarına uymayan ya da uysa bile haksız kazanç peşinde koşan misafirlere ise “düzenbaz” diyeceğiz. Kriptografik protokol düzenlemenin zorluğu da çoğunlukla, davete katılması engellenemeyen saldırgan ve düzenbazlara rağmen “dürüst” tarafların davetin amacına ulaşmasını sağlamaktır. Eğer herkes davetsiz ya da düzenbaz olursa ya da “ortam” davet düzenlemeye uygun değilse, davet elbette amacına ulaşamaz. Bu nedenle kriptografik protokollerde ortam ve katılımcılar üzerinde çeşitli varsayımlarımız olacak. Eğer varsayımlarımız gerçekçi değilse ya çok pahalı bir davet düzenleriz ya da kötü konuklar davetin altını üstüne getirir.

Resmi davetlerin farklı ülkeler arası ilişkileri güçlendirme, belli bir konuda katılımcıları bilinçlendirme gibi hedefleri vardır. Kriptografik protokollerse çoğu zaman aynı anda birçok hedefi sağlamaya çalışır. Veri gizliliği, veri bütünlüğü, kimlik doğrulama, kaynak doğrulama, inkâr ede-

Kripto protokollerinde de tıpkı resmi törenlerdeki protokollerde olduğu gibi davetliler, davetliler arasında hiyerarşi ve uyulması gereken katı kurallar vardır.



Visual Photos

dahale edemeyeceği bir hattan, örneğin kuantum kanalından) ya da güvensiz hattan (örneğin internetten) kriptografik tedbirlerle koruduktan sonra cihaza aracısız yollamasıdır. Peki, anahtar paketini koruyan anahtarlar güvenli bir şekilde nasıl iletilecek? Sonunda mutlaka bir anahtarın güvenli bir şekilde cihaza ulaştırılması gerekir.

Anahtar dağıtmadan, saldırgan da aradaki her mesajı dinliyorken, taraflar arasında taze ve rastsal bir anahtar oluşturabilir mi? İlk anda olanaksız gibi görünüyor. Gerçekten de ilk anahtar anlaşma protokolünün bulunuşu modern kriptolojide bir dönüm noktası olmuştur.

Anahtar anlaşmada kullanılan başka yöntemler de vardır. Bunlardan bir tanesi tarafların daha önceden paylaşılmış bir anahtarı doğrudan algoritmada kullanması yerine, bu anahtardan başka anahtarlar türetilmesidir. Bir diğer yöntem kullanılan anahtarın paydaşlar tarafından önceden bilinen bir fonksiyon ile güncellenmesidir. Bunun için genellikle tek yönlü fonksiyon kullanılır. Bu durumda eski anahtara dönülemediği için, güncel anahtar çalınsa bile hiç olmazsa eski mesajlaşmalar güvende olur.

Su Uyur Saldırgan Uyumaz

Saldırgan anahtarı bulduğunu çoğu zaman hissettirmez. Tedbir olarak anahtarları belli aralıklarla değiştirmemiz gerekir. Anahtarı değiştirme sıklığına anahtarı paylaşan taraf sayısı, anahtarın önemi, anahtar dağıtma maliyeti ve benzeri etkenler göz önüne alınarak karar verilir. Simetrik sistemlerde tek bir kişi bile paylaştığı anahtarı kaptırırsa diğerleri de kaptırmış olur. Bu nedenle çok kullanıcı sistemlerde mümkünse anahtar dağıtımında asimetrik şifreleme ya da taze anahtar oluşturma teknikleri kullanılmalıdır.

Ömrünü doldurmuş anahtarları cihazda saklamaya devam etmek de başka bir risktir, çünkü saldırgan anahtarı cihazdan ele geçirebilirse geçmiş mesajları inceleyebilir ya da anahtarın değiştiğinden haberi olmayan taraflarla mesajlaşabilir. Bu riski önlemek için ilk önce artık kullanılmayacak anahtarların silinmesi gerekir. Anahtarlar silinirken dikkatli olunmalıdır. Birçok kripto cihazı anahtarları silme işini işletim sistemine havale eder, fakat birçok işletim sisteminin silme işlemleri yeterince güvenilir değildir. Anahtar hafızada bir yerlerde siz farkında olmasanız da durmaya devam eder. Bu nedenle kripto sistemlerinde anahtarların imhası ve kullanılmayan anahtar bilgisinin cihaza kaydedilmesi, anahtar yönetiminin önemli bir parçasıdır.

Ele geçmiş ya da süresi dolmuş anahtarlardan diğer cihazların haberdar edilmesi de anahtar yönetiminde özen isteyen bir konudur.

mezlik ve anahtar anlaşma en çok ihtiyaç duyulanlardır. Bunlara son yıllarda önem kazanan mahremiyeti de eklemek gerekir.

Mahremiyet, bir işin kimin yaptığının sadece "gerekli kişiler" tarafından öğrenilmesi demektir. Bunun en çarpıcı örneğini elektronik gizli seçimden verebiliriz. Gizli seçimlerde, geçerli bir oyun kime verildiği belli olmalı fakat kimin tarafından verildiği belli olmamalıdır. Diğer bir deyişle, oy anonim olmalı ve oy verenin mahremiyeti korunmalıdır.

Elektronik oylama protokol tasarımının ne kadar güç olabileceğine güzel bir örnektir. Oy verenin kimliğinin gizlenmesi, oy verenin tekrar oy kullanamaması, oyların gerektiğinde tekrar sayılabilmesi, oy kullananın oyunun sayıldığından emin olabilmesi ve daha birçok hedefin aynı anda sağlanması beklenir. Bu hedeflerin hep birlikte sağlanması her zaman mümkün değildir. Bu nedenle çok uğraşılmasına rağmen herkesin gönül rahatlığıyla "tamam" diyebildiği bir e-oylama protokolü henüz bulunamamıştır. Belki yazımızı okuyanlardan birisi ileride bir çözüm bulur.

Arka Pencere

Bir senaryo üzerinden kriptografik protokolün önemini anlatmaya çalışalım. Alfred Hitchcock'un yönettiği "Arka Pencere" filmini görmüş müydünüz? İzlemediyseniz önemli değil. Sonunu söylemeyeceğiz ama senaryoyu biraz değiştiriyoruz. Örneğin başkahramanımız bir kadın. Haftalardır ayağı kırık bir şekilde, tekerlikli sandalyesinde oturan Ayşe can sıkıntısından evinin arka penceresinden etrafı gözetlemektedir. Ayşe bir gece karşı komşusunda korkunç bir olaya tanık olur. Komşusu evinin mutfağında ağır bir torba sürümektedir. Diğer taraftan komşunun karısı günlerdir ortalıkta gözükmemektedir. Ayşe cinayetten şüphelenerek dedektif Bora'yı aramaya karar verir. Ayşe'nin fazla vakti yok çünkü acele etmezse, komşusu delilleri yok edecek ve kaçacak. Önemli bir sorun daha var. Komşusu başkalarının hatlarından açık giden mesajları dinleyebilmekte ve dışarıda belalı arkadaşları kol gezmektedir.

Verdiğimiz örneğin, protokollerin (ya da kriptolojinin) önemini anlatmak için abartılı olduğunu iddia edebilirsiniz fakat gerçek hayatta düşman, hatları dinleyebiliyorken haberleşmeye çalışan askerler daha az tehlike altında değildir. Ya da ucunda ölüm olmayabilir ama "mal, canın yongasıdır" diyorsanız, güvensiz bir internet bankacılığı yüzünden aileniz bütün malvarlığını kaybedebilir.

Senaryodaki gibi günlük yaşamdaki kriptografik protokollerde de saldırganlar çoğu zaman dürüstlerden daha güçlü kuvvetli, yani işlem gücü çok daha yüksek ve daha beceriklidir. Ayrıca kim olduklarını tahmin edemediğimiz başka işbirlikçileri olabilir. Kriptologlar protokol ya da protokollerin yapıtaşlarını tasarlarken, kendilerini saldırgan yerine koyup buldukları çözümü alt etmeyi denerler. Saldırganın işlem gücünü, bilgisini ve işbirlikçilerini modelleyip buldukları çözümün güvenilir olduğunu ispatlamaya çalışırlar. Saldırgan modellemede en yaygın kullanılan modeller "standart" ve "(rastsal) kâhin" modelleridir.

Şimdi "Arka Pencere"mize geri dönelim. Amacımız Ayşe ile Bora arasında güvenli bir ihbar mekanizması kurmak. Bora'nın kötü niyetli olmadığını, örneğin katil zanlısı ile işbirliği yapmayacağını ve Ayşe'yi tanıdıktan sonra dediklerine kulak vereceğini varsayıyoruz. Protokolün sağlaması gereken hedefler arasında gizlilik, kimlik doğrulama ve veri bütünlüğünü korumanın yanı sıra mahremiyeti de sayabiliriz. Çünkü ihbarı kimin yaptığının komşunun arkadaşları tarafından anlaşılması Ayşe için can sıkıcı olurdu. Protokol ortamı, Ayşe ile Bora arasında telefon, cep telefonu veya internet hattı olabilir. Protokolün davetli misafirleri en azından Ayşe ile Bora. Davetsiz misafirler komşu ve işbirlikçileri.

Ne dersiniz; sizce Ayşe komşusunu yakalatabilecek mi?

Kaynaklar

Bogdanov, A. ve diğerleri, *PRESENT: An ultra lightweight block cipher*, CHES 2007, LNCS 7427, s.450-466, Springer, 2007.
Koblitz, N., *Algebraic Aspects of Cryptography*, Springer, Berlin, 1998.
Menezes, A. J., Oorschot, P.C. ve Vanston, S.A., *Handbook of Applied Cryptography*, CRC, NY, 1997.
Vaudenay, S., *A classical Introduction to Cryptography: Applications for Communications Security*, Springer, NY, 2006.
http://www.estream.org
http://www.iacr.org

Özellikle asimetrik sistemlerde imza anahtarının ele geçirildiğinin acilen bildirilmesi gerekir. Aksi takdirde saldırgan sizin adınıza geçerli imzalar atar. Elektronik ticarette birkaç günlük gecikmenin nelere yol açabileceğini siz düşünün!

Aslında anahtar yönetimi konusunda burada bahsedemediğimiz başka sorunlar da var. Örneğin imza sistemlerinde süresi dolmuş anahtarların kontrol edilmesi, açık anahtarların kullanıcılar ile ilişkilendirilmesi, geçmişe yönelik mesajların okunabilmesi için asimetrik şifreleme özel anahtarlarının arşivlenmesi, büyük gruplar için verimli anahtar oluşturma protokolü tasarlanması bunlardan sadece birkaçı.

Kripto algoritmamız sağlam. Anahtarı güzelce ürettik; sağ salim ulaştırdık; cihazın hafızasında korunaklı bir şekilde sakladık. Anahtarın yanlış kullanımını engelledik. Saldırgan anahtara cihazın içinde ya da hattan giden veriyi inceleyerek ulaşamıyor. Acaba anahtarımız güvende mi? Unutmayın saldırgan her yolu deneyecektir. Son yıllarda gelişen "yan kanal analizi" denilen yeni bir saldırı tekniği sayesinde saldırgan, cihazın kripto işlemleri sırasında harcanan zaman ve enerji gibi değerleri ölçerek anahtarı ortaya çıkarabiliyor. Yani algoritmamızın kriptoanalize karşı güvenli olması yetmez, aynı zamanda yan kanal analizlerine dayanıklı bir şekilde gerçeklenmesi gerekir.

Sağlam bir anahtar yönetiminin olduğu bir sistemde saldırgan ne anahtarı defolu üretiminden dolayı tahmin edebilir, ne saklandığı ya da "toprağa verildiği" yerden ele geçirebilir, ne taşıma ya da paylaşım sırasında çalabilir. Ne yazık ki, anahtar yönetimi anahtar güvenliği için mutlaka gerekli fakat tek başına yeterli değildir.

Kaynaklar

Koblitz, N., *Algebraic Aspects of Cryptography*, Springer, 1998.
Knuth, D., *The Art of Computer Programming*, Addison-Wesley, 1969.
Menezes, A. J., Oorschot, P. C., Vanston, S. A., *Handbook of Applied Cryptography*, CRC, 1997.
Vaudenay, S., *A Classical Introduction to Cryptography: Applications for Communications Security*, Springer, 2006.

*Uğur Kaşif Boyacı**

*Orhun Kara***

**Uzman Araştırmacı,*
***Dr., Başuzman Araştırmacı,*
UEKAE, TÜBİTAK

Bilgi Güvenliği Problemlerine Matematiksel Yaklaşım Getiren Bir Bilim Dalı

Kriptoloji

Düşmandan bilgi saklama ve gizli haberleşme insanoğlunun kafasını binlerce yıldır meşgul eden bir problem. Çok eski zamanlarda ilkel haberleşme teknolojisinden ve okuryazar oranının düşük olmasından faydalanılarak bu problemlere kolay çözümler getirilebilmiş. Oysa günümüzün son derece karmaşık ve gelişmiş bilgi ve haberleşme teknolojisinde, kimlik doğrulama, gizliliği sağlama, bilginin kaynağını doğrulama, verinin bütünlüğünü sağlama gibi bilgi güvenliği problemlerini çözmek o kadar kolay değil. Öyle ki, bu problemleri çözmek için bir bilim dalı doğmuş: Kriptoloji

Anahtar Kavramlar

Kriptoloji bir yandan gizlilik, veri bütünlüğü, kimlik doğrulama, inkâr edememe gibi bilgi güvenliği problemlerine matematiksel teknikler kullanarak çözüm getirme, bir yandan da bu çözümleri analiz etme ve çürütme bilimidir. Kriptografik bir çözüm oluşturmayı bir inşaata benzetirsek temel yapıtaşları, belli görevleri yerine getiren "algoritmalar"dır. Bu yapıtaşları çoğunlukla "anahtar"larla kullanılabilir.

Güvensiz bir kripto sistemi güvensiz bir uçak gibidir; ne kadar verimli olursa olsun, o sistemi kimse kullanmaz.

Eğer kripto algoritmanız güvenli ise saldırgan algoritma ile ilgili (algoritmanın işleyişi dahil, ama anahtar hariç) her şeyi bilse bile bir avantaj elde edemez.

Aslında pratikte kullanılan hemen hemen bütün sistemler kırılabilir. Ancak bunun bir maliyeti vardır ve bu maliyet çoğu kez insanlığın hiçbir zaman ulaşamayacağı kadar yüksektir.



Uğur Kaşif Boyacı, ODTÜ Matematik Bölümü'nden lisans derecesi ve Yıldız Teknik Üniversitesi Matematik Mühendisliği Bölümü'nden yüksek lisans derecesi aldı. Dizi şifreleme algoritmalarının analizi üzerine tez yazdı. Yaklaşık on yıldır kripto algoritmaları ve protokolleri üzerinde TÜBİTAK UEKAE'de çalışmaktadır.

Pek azımız kriptolojinin ne olduğunu, ne anlama geldiğini bilir. Aslında kriptoloji dünyanın en ilgi çekici ve gizemli bilimlerinden biridir. Biraz dar bir tanım olsa da, kriptolojiyi kısaca şifreleme ve şifre kırma bilimi olarak tarif edebiliriz.

"Şifre yapmanın ya da şifre kırmanın bilimi mi olur?" diye düşünebilirsiniz. Şifre kırma deyince büyük ihtimalle kafanızda, Hollywood filmlerinden çıkma cin gibi bir gencin telaş içinde, klavyede aynı anda bir sürü tuşa basarak FBI'ın giriş kodlarını ele geçirmesi canlanmıştır.

İnanın şifre yapmak ya da şifre kırmak sanıldığı kadar kolay bir iş değil. Sadece bu konuda çalışan profesörler bile var. Bu araştırmacılar saniyeler içinde klavyede yüzlerce tuşa basabilecek kadar hızlı değiller, ama aylar ve hatta yıllar süren çalışmalar sonucunda belli şifreleri çözmek için geliştirdikleri matematiksel yöntemlerle gerçek birer şifre kırıcılar.

>>>



Visual Photos

İnternetteki sohbet odalarında, biz farkına varmasak da kulak misafirlerimiz olabilir.

Kriptoloji kelimesinin kökü Eski Yunancadan gelir ve "gizem bilimi" anlamı taşır. Kriptolojiyi, bilgi güvenliği alanında matematiksel çözümler üreten ve bunları analiz eden bir bilim olarak düşünebiliriz. Kriptolojinin bilgi güvenliği sağlamak için çözüm üreten alt bilim dalına kriptografi, önerilmiş çözümleri analiz eden ve çürütmeye çalışan alt bilim dalına ise kriptoanaliz denir.

Kriptolojinin uğraşı alanlarını bir örnekle ifade etmek daha açıklayıcı olacaktır. Ankara'da bir kimya profesörü Zürih'teki bir ilaç firması için ilaç formülleri geliştiriyor olsun. Geliştirilen formüllerin firmanın Zürih'teki laboratuvarlarında test edilmesi gerekmektedir. Ya profesör belli aralıklarla Zürih'e gidecek ya da Zürih'ten Ankara'ya araştırmacılar gelecek. Bu görüşmeler sırasında profesör hazırlanan raporları elden teslim edecek ya da alacak. Firma yetkilileri geliştirilen yüzlerce formülün yolda kaybolabileceği endişesini taşıyor. Üstelik seyahat masrafları ve gecikmeler, firma için oldukça maliyetli olmaya başlamış. Başka ülkelerde ortak çalıştıkları diğer profesörleri de hesaba katınca seyahat masraflarının altından kalkılamaz hale geldiğini gören firma, bu duruma bir çözüm bulmaya karar veriyor. Seyahate ne gerek var? Zaten internet bilgileri kolayca transfer etmeye yaramıyor mu? Bunun üzerine, çalışanlar arasında formülleri paylaşmaları için sanal sohbet odaları kuruluyor. Böylece çalışanlar birbirlerine zahmetsizce yazı, ses ve görüntü iletme imkânına kavuşuyor.

İlaç firması raporları hızlı iletmenin yolunu buldu, ama güvenliği sağlayabildi mi? Muhtemelen hayır. Profesörümüzü internet ortamında bekleyen bir takım tehlikeler var. Profesör sanal sohbet odasında kendi firmasından arkadaşları ile sohbet ettiğini zannederken, aslında rakip ilaç firmasının araştırmacıları ile sohbet ediyor olabilir. Yani profesör sohbet ettiği kişilerin kimliğini doğrulayabilmeli. Bir diğer tehlike, rakip firmadakilerin sohbet odasında geçen konuşmalara "kulak misafi-

Şifreleme algoritmanızın sağlamlığı şifrelediğiniz metinleri kime karşı koruduğunuza bağlıdır. Eğer uzaylılar varsa ve galaksileri aşıp Dünya'yı ziyaret ettilerse, muhtemelen insanoğlunun modern şifrelerini kırabilecek hesapsal güce sahip teknolojiyi de geliştirmişlerdir.



Visual Photos

ri" olması. Formüller sadece profesör ve kimliğinden emin olduğu sohbet arkadaşları arasında gizli kalmalı. Rakip firmadakiler izlerini fark ettirmeden formülleri, gizli olsalar bile, değiştirebilir ya da bozabilir. Bunun önlenmesi için sohbet odasından giden verilerin bütünlüğünün sağlanması gerekir.

Yukarıda verilen örnekte bahsedilen problemleri çözsek dahi, bilgi güvenliğini tam olarak sağlamış sayılmayız. Daha verinin kaynağının doğrulanması, verilerin taze bilgi olduğunun yani daha önceki haberleşmeden kalma bilgi olmadığının doğrulanması, profesörümüzün ilaçlar kötü sonuç verirse "bunlar benim formüllerim değil ki" diye inkâr etmesinin önlenmesi gibi işler ve daha pek çok güvenlik problemi bizi bekliyor.

Kriptoloji, sayısal ortamda işte bu tür güvenlik problemleriyle uğraşan disiplinlerarası bir bilim dalıdır. Daha biçimsel bir tanım verecek olursak kriptoloji bir yandan gizlilik, veri bütünlüğü, kimlik doğrulama, inkârın önüne geçme gibi bilgi güvenliği problemlerine matematiksel teknikler kullanarak çözüm getirme, bir yandan da bu çözümleri analiz etme ve çürütme bilimidir.

Kriptografik bir çözüm oluşturmayı bir inşaata benzetirsek, temel yapıtaşları belli görevleri yerine getiren "algoritmalar"dır. Bu yapıtaşları çoğunlukla "anahtar"larla kullanılabilir. Sadece güçlü yapıtaşlarını kullanarak bir inşaat yapamayız. İnşaat için yapıtaşlarının belli bir plan-proje çerçevesinde, belli sırayla, belli kişiler tarafından bir araya getirilmesi gerekir. Bu plan ve iş kurallarına "protokol" denir.

Kriptoanaliz Nedir?

Bütün kripto algoritmalarından, protokollerinden ve uygulamalarından mühendislik açısından iki temel özelliğe sahip olmaları beklenir: Güvenlik ve verimlilik. Bu iki gerekliliği sıraya koymak gerekirse, önce gelen güvenliktir. Güvensiz bir kripto sistemi güvensiz bir uçak gibidir; ne kadar verim-

>>>

li olursa olsun, kimse kullanmaz. Sesten birkaç kat hızlı bir uçak tasarlayın. Emin olun, uçağınız güvenli değilse, Ankara'dan New York'a iki saatte varsa bile, kimse onunla uçmayacaktır.

Algoritmaların verimliliği, genel olarak kriptonun çalışacağı platformdaki hızı, hafızada ya da devre şemasında kapı sayısı olarak kapladığı yer ve tükettiği güç ile ölçülür. Uygulama platformunun kısıtlarına göre bu kıstaslardan bazıları öne çıkar. Örneğin RFID etiketlerinde koşacak bir algoritmanın kısıtlı yonga alanı nedeniyle az yer kaplaması ve etiketlerin dışarıdan yani elektromanyetik ortamdan elde ettikleri enerjiyi tüketmelerinden dolayı az güç harcaması gerekir. Burada hız ikinci planda kalır.

Çok çeşitli RFID etiketleri vardır, ama genel olarak RFID etiketlerini mağazalarda ürünlere yapıştırılan ve kapıda alarmları çaldıran, içinde labirent gibi, sarmal şeklinde bir antenle sarılmış küçücük bir yongadan oluşan etiketler olarak düşünebilirsiniz. Kutusuna RFID etiketi yapıştırılmış bir ürün aldığınızda (örneğin bir DVD filmi) etiketi kutudan ayırın. İçindeki labirent gibi anteni sökün. Masrafsız bir şekilde bozup kurcalamanın tadını çıkarın. Büyütecinizle antenin ortasındaki küçücük yongayı yakından inceleyin. O yongada bir kripto algoritmasının koştuğunu hayal edin ve bu algoritmanın şifrelediği metinleri milyarlarca TL'lik süper-bilgisayarların bile çözemediğini düşünün.

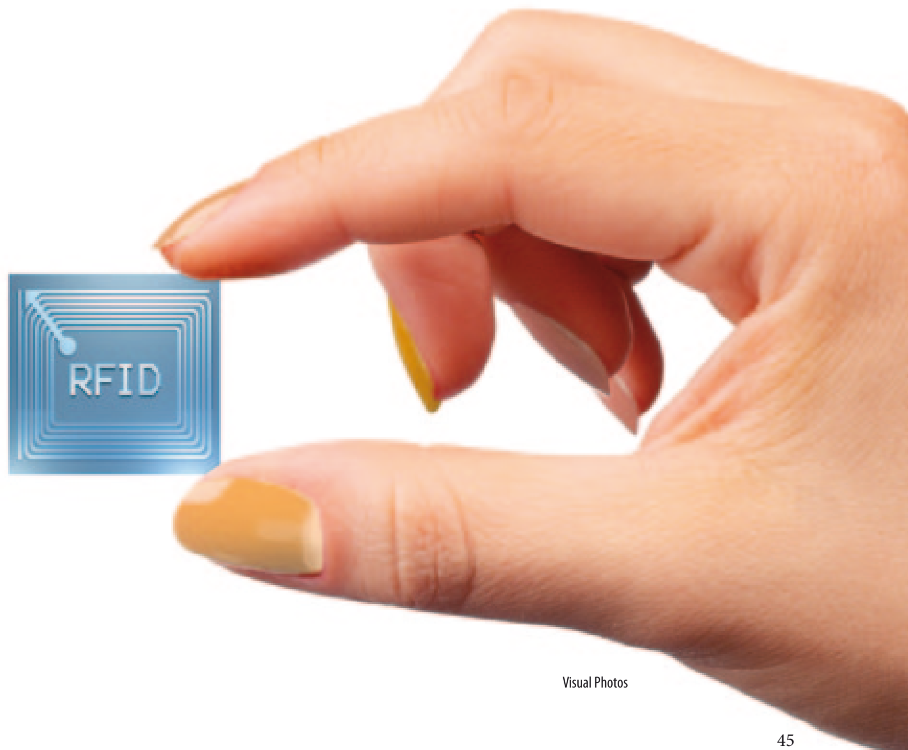
Algoritmaların güvenliğini ölçmek son derece zordur ve ayrı bir uzmanlık gerektirir. Bir algoritmanın ne kadar güvenli olduğu algoritmayı kırmaya çalışan varlığın entelektüelliği ile ilgilidir. Yani insanoğlu akıllı bir varlık olan insanoğluna karşı önlem almaya çalışmaktadır.

Mühendisliğin birçok alanında güvenlik problemleri çok daha açık ve nettir. Köprü, bina ya da tünel yapımında mühendisler zor hava şartlarına ya da depreme karşı nasıl önlem alacaklarını hesaplayabilir. En zorlu koşullara göre tasarımlarını yaparlar ve bu koşullardan daha zorlu koşullarla karşılaşmayacaklarından emin olabilirler. Oysa kripto algoritma ya da protokol tasarımında tehditler belirsiz olduğundan alınacak önlemler de açık değildir. İşte güvenli bir kripto sistemi tasarlamanın altında yatan kavramsal zorluk buradan gelir. Yıllarca güvenli olduğu düşünülen bir şifreleme algoritması, yeni çıkan bir saldırı metoduna maruz kalarak bir günde güvensiz hale gelebilir. Dünyanın en tanınmış ve önde gelen kriptologlarının protokol tasarımları bile kırılabilir. Literatür bu tür örneklerle doludur. Diğer tasarım bilimlerinde pek rastlanmayan bu olguyla kriptografide sık sık karşılaşırız.

Kripto algoritmalarının güvenliğini ölçme bilimine kriptoanaliz denir. Bir algoritmanın güvenliğini ölçmek, o algoritmanın ne kadar sağlam olduğunu ispatlamak gibi pozitif yönde olabileceği gibi, algoritmayı kırmak gibi negatif yönde de olabilir. Genellikle kriptoanaliz negatif yönde çalışmalarla, yani kripto sistemlerini kırmakla özdeşleşmiştir. Halbuki bir kripto sisteminin güvenliği hakkında yapılan her çalışma, olumlu olumsuz elde edilen her sonuç, bir kriptoanaliz faaliyetidir..

Bir kriptolog tasarladığı algoritmanın ne kadar sağlam olduğunu matematiksel ya da biçimsel olarak kanıtlama yoluna gidebilir. Bu yönde yaptığı çalışmalar ve algoritmasının sağlamlığı ile ilgili elde ettiği bulgular, kendi tasarımı için bir kriptoanaliz çalışması demektir. Güvenlik ispatı yapılırken önce genellikle olası saldırganın kabiliyeti modellenir. En yaygın kullanılan modellemeler "standart" ve "kâhin" modellemeleridir.

Aslında kullanılan hemen hemen bütün sistemler pratikte kırılabilir. Ancak bunun bir maliyeti vardır ve bu maliyet de çoğu kez insanlığın hiçbir zaman ulaşamayacağı kadar yüksektir. Diğer taraftan, teoride kırılamayacağı ispatlanabilen şifreler vardır. Örneğin 1918'de bir AT&T mühendisi olan Vernam'ın önerdiği Tek Kullanımlık Istampa (OTP-*One Time Pad*) şifrelemesinin, 1949'da başka bir AT&T mühendisi Shannon tarafından şartsız güvenlik sağladığı ispatlanmıştır. Düşmanın sonsuz bir hesaplama gücü olsa bile, şifreyi kırması mümkün değildir. Ancak şifreleme için açık me-



Bir RFID etiketi

Visual Photos

tin kadar bir anahtar da gerektiğinden ve bir anahtarla sadece bir kere şifreleme yapılabildiğinden, Vernam'ın tek kullanımlık ıstampası pratik değildir. İlginç olan, bu şartlar sağlanmadığı zaman Vernam şifrelemesinin son derece zayıf kalmasıdır.

Kriptologlar şartsız güvenlik yerine, uygulaması çok daha kolay olan hesapsal güvenliğe yoğunlaşır. Günümüzde hemen hemen bütün kripto sistemleri ve algoritmaları bu güvenlik kriterine göre tasarlanır. Hesapsal güvenliğe göre tasarlanmış bir algoritmanın sağladığı güvenlik, belirlenmiş bir hesapsal zorluk ile ifade edilir. Bu zorluğu aşacak hesapsal güce sahip olanlar sistemi kırabilir.

Hesapsal zorluk derecesi genellikle günümüz teknolojisiyle, hatta 50-100 yıl sonrasının teknolojisiyle dahi ulaşılamayacak bir hesapsal güç gerektirecek şekilde belirlenir. Örneğin bir şifreleme standardı olan AES şifreleme algoritması, en düşük seviyede 128 bitlik, en yüksek seviyede 256 bitlik güvenlik sağlar. Kaba kuvvet (yani anahtarları tek tek deneme) saldırısı ile 2'nin 128. kuvveti kadar (yani 128 tane 2'nin çarpımı kadar) şifreleme yapmak, günümüz teknolojisi ile ve hatta 15-20 yıl sonrasının teknolojisiyle bile, hesaplama biliminde çok önemli bir gelişme olmayacağını varsayarsak, mümkün gözükmemektedir. Bu hesapsal güce kimsenin ulaşamayacağını kabul edersek, AES kaba kuvvet saldırısına dayanıklıdır. Ama tabii kimbilir, belki uzaylılar vardır ve onların teknolojileri çok daha gelişmiştir. Bu uzaylılar belki kuantum bilgisayar da imal etmiş olabilir ve insanoğlunun AES ile yaptığı şifrelemeleri çözebiliyorlardır. Hesapsal güvenlikte, düşmanın hem günümüzdeki hem de gelecekteki hesapsal gücünü dikkate almak ve teknolojinin geleceğini öngörmek gerekir.

Güvenlik İspatında Kâhin Modeli

Tipilere ve hırçın rüzgârlara meydan okuyup yalçın kayalıkların arasındaki, bulutlara tepeden bakan mağaraya ulaştınız. Ulu kâhinin huzuruna çıkıyorsunuz. Size kâhinin soracağınız tüm sorulara cevap vereceği müjdelendi. Yalnız asıl cevabını aradığınız soru hariç: Mutluluğun anahtarı nedir?

İşte, kriptografik ispatlarda saldırganın yeteneğini modellemekte en çok kullanılan yöntemlerden biri de saldırganın böyle bir bilgeye danıştığı varsayımını kabullenen "Rastsal Kâhin Modeli"dir (random oracle model). Efsanedeki kâhin her şeyi bilse de, rastsal kâhinin bilgisi sınırlıdır.

Kâhinin huzurunda soru sormanın adabı nedir?

Başlıca kuralları sıralayalım: Kâhine doğrudan aranan cevabı verecek (örneğin "bu algoritmanın anahtarının tersi nedir?" ya da "Sayın kâhin, bana şu özet fonksiyonunda bir çakışma verir misiniz?" gibi) sorular sorulamaz. Kâhinden bilmediği soruların cevabı beklenmez. Örneğin kâhin sadece özet alabiliyorsa, özet çıktıya bakıp giren metni söylemesi beklenmez. Aynı sorunun birden fazla cevabı varsa, kâhin aynı soruya hep aynı cevabı verir. Örneğin bir fonksiyon çıktısına giden farklı girdi değerleri arasından hep aynısını seçer, fakat siz hangi cevabı vereceğini ilk soruyu sormadan tahmin edemezsiniz. Çünkü ilk seçim rastsaldır.

Kâhin modelinin kullanılışına bir örnek verebilir misiniz?

Diyelim ki, bir blok şifreleme algoritmasının anahtarını ele geçirmek istiyorsunuz. Kâhine istediğiniz açık metinlerin şifreli karşılığını sorabilirsiniz. Hatta seçtiğiniz şifreli metinlere karşılık gelen açık metinleri de sorabilirsiniz. Daha da ileri gidip, seçtiğiniz bazı özel açık metin çiftlerinin (örneğin sadece bir karakteri farklı, açık metin çiftleri) şifreli karşılığını isteyip, sonra bu şifreli metin çiftlerindeki eşlerden her birinin birer karakterlerinin değiştirilmiş hallerine karşılık gelen açık metinleri de isteyebilirsiniz. Kâhinden öğrendiğiniz açık-kapalı metin çiftlerini analiz edip

JUPITERIMAGES

Aslında şu ana kadar bir kripto sistemini kırmanın ne anlama geldiğini henüz açıklamadık. Bir kripto sistemini kırmak, belirlenmiş bir hesaplama gücüne karşı sağlandığı iddia edilen bir kripto hizmetinin, daha az hesaplama gücüyle engellenmesi olarak tanımlanabilir. Belki kısa bir yol vardır; AES'i kırmak için 2'nin 128. kuvveti kadar şifreleme yapmaya gerek olmayabilir. Kim bilebilir ki! AES on yıldır literatürde olmasına ve yoğun kriptoanaliz çalışmalarına maruz kalmasına rağmen, cak atağı uygulamak pratikte mümkün olmayabilir. Bir AES şifrelemesinde kullanılmış anahtarı 2'nin 120. kuvveti kadar şifreleme yaparak ele geçirecek bir yöntem keşfetmiş olabilirsiniz. Bu durumda AES'i kırmış sayılırsınız. Kripto dünyasında meşhur olursunuz ve kripto tarihine geçersiniz. Ancak AES'in sağlaması gereken hesapsal güvenliği 256 kat aşağı çekmiş olsanız dahi, atağınız pratikte uygulanamayacaktır. 2'nin 120. kuvveti kadar şifreleme yapabilecek teknolojiyi elde

buradan anahtarı tahmin etmeye çalışırsınız. Hâlâ anahtarı ele geçirecek bir yöntem aklınıza gelmiyorsa, algoritmanın sağlam olduğuna kanaat getirebilirsiniz. Bu kanaatiniz henüz bir teorem değil. Eğer anahtarın ele geçirilemeyeceğine dair bir ispatınız varsa, o zaman başka. Bu durumda kâhin modeliyle güvenlik ispatı yapmış olursunuz.

Kâhin modeli ne kadar "gerçekçi"?

Saldırganın ele geçirdiği, içini açıp anahtara ulaşamasa da istediği mesajları şifreleyebildiği bir kripto cihazını, pratik bir şifreleme kâhini olarak düşünebiliriz. Ayrıca saldırganlar sistemin işleyişini, anahtar hariç, biliyor.

Peki saldırgan kâhine danışabiliyorsa anahtara ne ihtiyacı var?

Dağın tepesindeki bir ölümlü, kâhini sürekli meşgul edemez.
Hem kâhine danışmanın bedava olduğunu kim söyledi? Saldırganın başarısı, kâhine en az sayıda ve niteliği düşük soru sorarak elde etmek istediği sonuca ulaşmakta. Örneğin toptan sorulan n tane soru, her biri eski cevaplardan faydalanılarak sorulan n tane soruya göre daha düşük niteliklidir.

Bir sistem rastsal kâhin sayesinde de çözülemiyorsa güvenli midir?

Kâhin modeli benimsenerek güvenliği ispatlanmış kripto algoritmaları ve protokolleri, bir tür zorlu şartlara dayanıklılık testinden geçmiş gibi algılanabilir. Ama dikkat!
Kriptoloji son derece şaşırtıcı bir bilim. Zorlu teorik koşullarda sağlamlığı kanıtlanmış bir algoritma, pratik hayatta çok daha basit koşullarda güvensiz olabiliyor. Literatürde kâhin modeli benimsenerek güvenliği belli koşullarda ispatlanmış ama ardından pratik saldırılarla kırılmış kripto algoritmalarına ve protokollerine rastlayabilirsiniz.

Bu neden kaynaklanıyor?

Rastsal kâhin çoğu zaman ideal fonksiyonlar kullanıyor. Örneğin özet fonksiyonu gerçekten olması gerektiği gibi, fakat pratik sistemlerde bu tür fonksiyonların çok ufak da olsa kusurları olabiliyor. Ayrıca ispatlardaki varsayımlar, gerçek hayatta rastlayamayacağımız kadar "uçuk" olabilir.

O zaman ispatlarda kâhin modeli neden kullanılıyor?

Bu soru kriptologlar arasında da çok tartışılıyor. Saldırganın sadece işlem gücü ve sorgu sayısı ile sınırlandığı standart modelde ispat yapmak son derece güç, hatta bazı durumlarda imkânsız gibi. Çoğunlukla ispata nereden başlanacağı bile bilinmiyor. Hiç ispatı olmayan bir sistem yerine rastsal kâhine dayanıklı bir sisteme daha çok güvenebiliriz, çünkü pratikte kusurlu parçaları değiştirebiliyorsanız saldırganın eli kolu bağlı demektir.
Hem kriptologlar her geçen gün daha dayanıklı parça üretmenin yolunu öğreniyor. İleride kusurlu tarafları düzelterek, pratikte de güvenli bir kripto sistemine ulaşılabilir.

şu ana kadar daha kısa bir yol bulan çıkmadı. İşin ilginç yanı, daha kısa bir yolun olmadığını ispatlayan da çıkmadı.

Yukarıda verdiğimiz kripto sistemi kırma tanımı teorik bir tanımdır. Bir kripto sistemindeki hiç hesapta olmayan, o ana kadar kimsenin fark edemediği bir özellikten kaynaklanan bir zayıflığın sömürülmesiyle o sistem kırılmış sayılabilir. Ancak etmek (bunun için milyarlarca TL harcamaya hazır olsanız dahi) şu anda ve yakın gelecekte mümkün gözükmüyor.

Kaynaklar

Kahn, D., *The Codebreakers: The Story of Secret Writing,* Scribner, 1996.
Koblitz, N., *Algebraic Aspects of Cryptography,* Springer, 1998.
Mel, H. X., Baker, D., *Cryptography Decrypted,* Addison Wesley, 2001.
Menezes, A. J., Oorschot, P. C., Vanston, S. A., *Handbook of Applied Cryptography*, CRC, 1997.
Vaudenay, S., *A Classical Introduction to Cryptography: Applications for Communications Security*, Springer, 2006.

Gündelik Hayatta Kriptoloji

Teknolojik ürünlerin gündelik hayatımızın bir parçası haline geldiği günümüzde, pek çok değerli varlığımız sayısal bir bilgi bulutu halinde etrafımızı çevreliyor. Yolda yürürken cep telefonumuzdan bankamıza erişebiliyor, yol haritalarını takip edebiliyor, ihtiyacımız olan anlık bilgilere talep ettiğimiz anda ulaşabiliyoruz. Sağlık verileri gibi şahsi bilgilerin yanı sıra, kurumların önemli bilgileri de bu bulutta yerlerini çoktan aldılar. Bu bilgilerin gelişen teknoloji ile herkes tarafından ulaşılabilir hale gelmesiyle bilgilerin güvenliği konu oldu. Uzmanlar uzun zamandan beri bu bilgilerin korunması için kriptoloji kullanıyorlar. Peki, nerede bu kriptoloji?

Anahtar Kavramlar

Gündelik hayatta kullandığımız cep telefonları kriptolu haberleşme yapmaktadır.

Güvenli olduğu zannedilen bazı uzaktan kumandalı araç alarm ve çalıştırma anahtarlarında kullanılan kriptografik yapılar kırılarak bu anahtarların kopyalarının üretilebildiği 2008 yılında bir grup araştırıcı tarafından gösterildi.

Yaygınlaşan RFID teknolojisinin yarattığı mahremiyet endişesine kriptoloji çözüm vaat etmektedir.



A. Murat Apohan, doktora derecesini İstanbul Teknik Üniversitesi'nden almıştır. NATO kripto ve bilgi güvenliği çalışma gruplarında yer almıştır. TÜBİTAK UEKAE Kriptoloji Bölümü sorumlusu olarak görev yapmaktadır. 2007-2008 yıllarında Uluslararası Kriptoloji Organizasyonu'nun (www.iacr.org) yönetim kurulunda yer almıştır.

Sıradan teknoloji kullanıcısı kriptoloji ile karşı karşıya olduğunu ancak bazı ipuçlarından anlayabilir. Size kullanıcı şifresi soran bir internet sitesi, evde kurmaya çalıştığınız kablosuz ağ bağlantısı için istenen şifre veya kredi kartınızı kullanırken sorulan şifre, sahnenin arkasında oluşturulması yüzyıllara yayılmış güncel matematiğin en derin konularını kullanan kriptolojinin varlığına dair ilk işaretlerdir. Kriptoloji aslında gündelik hayatımızın her yerinde: cebimizdeki çipli banka kartında, otomobil anahtarında, internet üzerinden yaptığımız bankacılık işlemlerinde, kablosuz ağlarda, cep telefonlarımızda, DVD'lerin kopya korumasında, kısaca değerli bilginin olduğu her yerde.

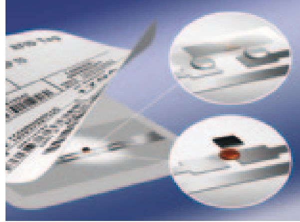
Kriptoloji günümüzde askeri haberleşme, komuta kontrol ve karmaşık silah sistemlerinin de vazgeçilmez bir parçası haline gelmiştir. Savaş uçakları dostu düşmanı yüzlerce kilometre uzaktan kriptoloji sayesinde ayırt ederken, pilotun silah kullanmaya yetkisi olup olmadığını kriptografik metotlarla denetlemektedir. Zaman içinde diğer askeri teknolojilerde olduğu gibi kriptoloji de sıradan vatandaşın gündelik hayatına girmiş ve bu konuda öncü teknoloji internet olmuştur. İnternetin yaygınlaşması ile banka şubeleri bilgisayarlarımıza taşınmış ve bankadaki paralarımızın sanal karşılığı olan sayıların korunması gerekmiştir. Bu amaçla kullanılan ilk kripto protokolü NETSCAPE firması tarafından geliştirilen SSL olmuştur. Ancak o dönemde ABD'nin uyguladığı güçlü kriptonun yayılmasını engelleyen kurallar gereği, SSL kripto protokolündeki şifreleme algoritması düşük anahtar boyu ile kullanılmıştır. Bunun sonucunda Andrew Twyman isimli bir öğrenci 1996 yılında, bağlantı başına 584 dolar maliyet ile bu sistemin kırılabileceğini göstermiştir. Kriptologların çalışmaları ile bu protokol oldukça güvenilir bir hale gelmiş ve TLS ismi ile bankacılık işlemlerinde temel güvenlik bileşenlerinden biri olmuştur.



Güçlü kriptoya sahip bir cep telefonu

> <

Kriptolojinin yer aldığı ve gündelik hayatta karşılaştığımız bir başka uygulamaysa cep telefonlarıdır. Neredeyse bir parçamız haline gelen cep telefonumuzun aslında kriptolu bir telefon olduğunu pek azımız biliriz. Cep telefonu ile baz istasyonu arasındaki haberleşme, yapılan görüşmelerin yetkisiz kişilerce dinlenmesini engellemek amacıyla GSM standartları doğrultusunda A5/1 (ABD ve Avrupa kullanımına özel), A5/2 (ABD ihraç izinleri çerçevesinde kullanılmak üzere zayıflatılmış algoritma) veya A5/3 (3G standardı için özel algoritma) isimli algoritmalardan birisi kullanılarak şifrelenir. Kriptologların çalışmaları ile A5/1 ve A5/2'nin yetersiz olduğu gösterilmiştir. A5/3 ise sıradan bir kişiyi meraklı kulaklardan uzak tutacak kadar güce sahiptir. Ancak bu sistemlerin hiçbiri güçlü bir kripto analiz grubuna karşı bir cep telefonundan diğerine kadar güvenli bir kanal oluşturmak için yeterli değildir. Bu nedenle aktarılan bilgilerin gizliliğinin yüksek olduğu yerlerde çok güçlü kripto algoritmalarına ve anahtar yönetimine sahip özel tasarlanmış haberleşme sistemleri kullanılır.


RFID etiket

Kriptoloji eğlence hayatımıza da girmiştir. DVD'lerde kullanılan kopya koruma sistemi de kriptografik tekniklere dayanmakta olup burada da kripto tasarımcıları ile kripto analizciler arasında bir rekabet süregitmektedir. DVD'lerde kullanılan içerik koruma sistemleri hedeflenen başarıyı gösterememiştir. Bunun temel sebeplerinden biri kriptolojide bulunan karmaşık yapıların yarattığı güven zincirinin son halkası olan kripto anahtarını koruyacak yapıların uygun bir biçimde oluşturulmamış olmasıdır. Bu sistemlerde tersine mühendislik yöntemleri ile kriptografik anahtarlar ele geçirilebilmiş ve kopya koruma özelliği kaldırılabilmiştir.

Peki kriptolojide güvenin temel dayanağı olan kripto anahtarlarını nasıl koruyacağız? Gündelik hayatta kripto anahtarlarını korumayı başarabilen en gelişkin sistem çipli banka kartlarıdır. Banka kartı, bizim hesap sahibi olduğumuzu bankaya ispatlamada kullandığımız araçtır. Kartın görevi ise yeterince uzun bir kriptografik anahtarın güvenli olarak saklanmasını sağlamaktır. Bir işlem sırasında kart bu anahtara sahip olduğunu bankaya ispatlar, bu da kart sahibi olan bizim yetkili kişi olduğumuzu gösterir. Burada önemli olan karttaki anahtarın üçüncü şahısların eline geçmesinin engellenmesidir. Geçmiş dönemlerde kullanılan manyetik kartlarda saklanan bu bilgiler basit bir kopyalayıcı ile ele geçirilebiliyorken, günümüz çipli kartlarının sahip oldukları güvenlik mekanizmaları içeriklerini kopyalamayı imkânsız hale getiremese de, iyi tasarlanmış bir kart için oldukça güç ve yüksek maliyetli bir işlem olur. Akıllı kartlar banka kartlarının yanı sıra kimlik, pasaport, ehliyet gibi kimlik sistemlerinde de yer almaya başlamıştır. Kripto tasarımı ile analizi arasındaki mücadele biz farkında olmasak bile cebimizde devam etmektedir.

Kriptografi bize güvenlik desteğinin yanı sıra beklemediğimiz bazı kolaylıklar da sağlamıştır. Örneğin tükenmez kalemle attığımız imzalar, bilgilerin kâğıttan dijital ortama kayması ile yerini dijital imzaya bırakmıştır. Mürekkepsiz imza! Sayısal imza asimetrik kriptonun bize sunduğu bir imkânı kullanır. Çok basitçe sayısal imzayı açıklamak istersek: şifreleme ve şifre çözme anahtarlarının birbirinden farklı olması bir mesajı sadece bizim sahip olduğumuz bir anahtarla (imza anahtarı) şifrelememizi sağlar. Herkesin kolayca erişebildiği ikinci anahtar (imza kontrol anahtarı) ise bu mesajın açılabilmesini ve imzanın bizim tarafımızdan atıldığının teyit edilmesini sağlar. Günümüzde gerekli yasal düzenlemelerin yapılması ile elektronik imza kullanılmaya başlanmıştır. Bu sayede elektronik yolla aldığımız belgeler ıslak imzalı kâğıt belgeler gibi hukuki geçerliliğe sahip olur ve kâğıt tasarrufu sağlanabilir.

Teknolojinin gelişimi ile ürünlerde kâğıt etiketler yerine elektronik etiketler kullanılmasıyla kriptografi mağaza raflarında da görülmeye başlandı. Bu etiketlerle, üründen çıkarılması unutulduğunda çalan alarmlar sebebiyle belki tanışmışızdır. Bu etiketler ürünle ilgili bilgileri kablosuz haberleşme kullanarak sorgu cihazına iletir. Bu sayede ürünle ilgili bilgilere uzaktan erişilebilir. RFID teknolojisi sayesinde çamaşır makinesi, içindeki giysinin etiketini okuyup doğru programı seçebilir, buzdolabı sakladığı ürünlerin son kullanma tarihlerini denetleyip uyarı verebilir, pasaportlar uzaktan okutularak sınır kapılarından geçilebilir, uzaktan ödeme ve binlerce ürünün bulunduğu bir ambarda hızlı stok sayımı yapılabilir. Ancak bu sistem, etiketleri taşıyan ürünlerin uzaktan izlenebilmesi nedeniyle önemli bir mahremiyet endişesi de yaratmıştır. Bir okuyucu ile bir kişinin üzerinde taşıdığı bu yolla etiketlenmiş bütün ürünleri izlemek mümkün olabilir. Bu noktada da kriptoloji devreye girerek bu etiketlerin sadece yetkili okuyucular tarafından sorgulanabilmesini sağlamaktadır.

Özetle biz farkında olmasak bile, bizi çevreleyen ve etrafımızla iletişim halinde kalmamızı sağlayan elektronik dünyanın güvenli ve güvenilir kalmasını kriptoloji sağlamaktadır.

Kaynaklar
Menezes, A., *Handbook of Applied Cryptography*, CRC Press, 1996.
Indesteege, S., Keller N., Dunkelman O., Biham E., Preneel, B., "A Practical Attack on KeeLoq", www.iacr.org/conferences/eurocrypt2008/.
Garfinkel, S. ve Rosenberg, B. (ed.) *RFID: Applications, Security, and Privacy*, ISBD-ISSN 032190968.
Barkan, E., Biham E., Keller, N., "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Technion - Computer Science Department, Technical Report CS-2006-07 – 2006.
http://www.akiskart.com.tr

Mini Bilgisayarlar: Akıllı Kartlar

Bellek, işlemci, dış dünya ile bağlantıyı sağlayan arayüz ve bir işletim sistemine sahip olan akıllı kartlar her gün karşılaştığımız bilgisayarların ölçek ve kapasite olarak küçük bir modelidir. Peki bu hesaplama gücüne neden ihtiyaç duyuluyor? Sonuçta bu kartlardan beklenen, kripto anahtarı denilen ortalama birkaç yüz bit uzunluğundaki bir veriyi saklaması ve ihtiyaç duyulduğunda doğru anahtara sahip olduğunu ispatlamasıdır. Bu basit işlem neden böylesine karmaşık bir yapı gerektiriyor? Zorluk özel kripto anahtarının kimseye verilmemesi gereğinden doğar. Eğer bir kez bu karttan çıkarılıp kopyalanabilirse, bu anahtarı kopyalayan kişi artık bu anahtarın asıl sahibinin kimliğine sahip olmuş olur. Bu nedenle akıllı kartlar, bu anahtar yerine, kriptografik olarak kendisine yöneltilen sorgu bit dizisine karşılık bu anahtarı ve bu sorguyu kriptografik bazı algoritmalara girdi yaparak hesapladığı bir sayı dizisini verir. Böylece anahtarı korumuş olur. Bu işlemler belirli bir hesaplama gücü gerektirir. Bu nedenle bu kartlar bir mini bilgisayara dönüşmüştür. Günümüzün çipli kartları sahip oldukları yüksek güvenlik önlemlerine rağmen eğer gerekli tedbirler alınmamış ise yan kanal saldırıları denilen saldırılara maruz kalabilirler. Bu saldırılar kartların kriptografik işlem yaparken harcadıkları güç, zaman vb bilgileri kullanarak sakladıkları anahtarları hesaplamayı hedefler. Ancak kart tasarımcıları bu saldırılara karşı da önlem alır.



Milli işletim sistemli ve çipli akıllı vatandaşlık kartı

Kara Kutu mu, Şeffaf Kutu mu?

Geleneksel olarak kriptografik bir cihaz iç işleyişi bilinmeyen, girdiler, çıktılar ve transfer algoritmasından oluşan bir karakutu olarak görülür. Kötü niyetli bir kişinin elinde girdiler, çıktılar veya girdi-çıktı ikilileri hakkında birtakım bilgiler olsa bile, gizli anahtarı bilmeden saklanan bilgiyi deşifre etmesinin mümkün olmadığı düşünülür. Kriptografik algoritmaya karşı bilinen tüm saldırıları olanaksız hale getirecek büyüklükte bir anahtar seçtikten sonra kuramsal olarak güvenli bir şifreleme sistemi oluşturmuş oluruz. Bu güvenlik tanımı, kötü niyetli kişilerin kriptografik cihazlara sadece karakutu olarak erişebileceği varsayımı üzerine kuruludur. Bu nedenle karakutu yaklaşımı ile tasarlanan bir sistemin sadece kuramsal olarak güvenli olduğunu söyleyebiliriz. Oysa gerçek hayatta kriptografik cihazlar, fiziksel yan kanallar yoluyla iç işleyişleri hakkında bilgi edinilebilen, kara değil şeffaf kutulardır.

Anahtar Kavramlar

Yan kanal: Kriptografik bir cihazın, iç işleyişi hakkında bilgi sızdırılmasına yol açan fiziksel özellikleri

Yan kanal analizi: Kriptografik cihazların fiziksel özellikleri yolu ile gizli tutulması gereken iç işleyişleri hakkında bilgi edinilmesi

Kriptoanaliz: Şifreleri ve kriptogramları analiz etme ve çözme bilimi



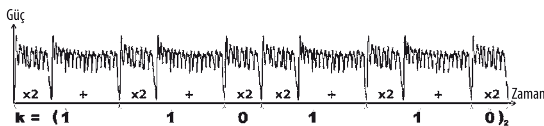
Deniz Karakoyunlu, 1999 yılında İzmir Fen Lisesi'nden mezun oldu. Lisans eğitimini 2004 yılında Sabancı Üniversitesi'nin Mikroelektronik Mühendisliği Bölümü'nde tamamladıktan sonra, ABD'nin Massachusetts eyaletinde bulunan Worcester Politeknik Enstitüsü'nün Elektronik ve Bilgisayar Mühendisliği Bölümü'nde yüksek lisans eğitimine devam etti. 2007 yılında yüksek lisans diplomasını almaya hak kazanan Karakoyunlu, halen Worcester Politeknik Enstitüsü bünyesindeki Kriptografi ve Enformasyon Güvenliği Laboratuvarı'nda doktora çalışmalarına devam ediyor. İlgi alanları kriptografik donanım tasarımı, yan kanal analizi, yüksek verimli kriptografik mimariler ve aritmetik algoritmalardır.

Matematiksel olarak tam güvenlik sağlamak, bir cihazın fiziksel işleyişinin de güvenli olduğu anlamına gelmeyebilir. Yani güvenli olduğu düşünülen karakutu, iç işleyişi hakkında bilgi sızdırıyor olabilir. Yan kanallar yolu ile edinilen bilgi kriptografik cihazın güvenlik tanımını tamamıyla geçersiz kılabileceği gibi, kısmi bilgi sağlayarak imkân dahilinde olmayan saldırıları da olası hale getirebilir. Yan kanal yolu ile elde edilen bilgiler, sistem güvenliğini sadece % 1 oranında azaltsa bile, bu sistemin kullanılamaz hale gelmesi demektir. Bir elektronik cihazın % 99 oranında çalışması performans değerlendirmesi açısından kabul edilebilir olabilir. Oysa bir kriptografik cihazın % 99 oranında güvenli olması güvensiz olduğu anlamına gelir. Bu nedenle, kriptografik cihazların her koşulda % 100 güvenlik sağladığından emin olabilmek için fiziksel işleyiş sırasında sızdırılan bilgileri de dikkate almak gerekir.


JUPITERIMAGES

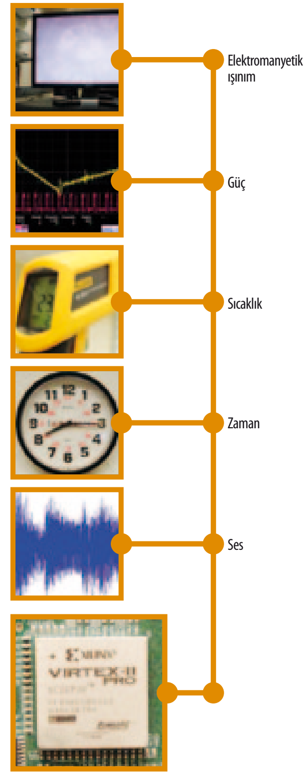
Peki, nedir bu bilgi kaçağına yol açan yan kanallar? İsminden de anlaşılacağı gibi, bir sistem hakkında bilgi sızdıran ve tasarım aşamasında öngörülemeyen kanallardır. İlk olarak 1996 yılında Paul Kocher tarafından öne sürülen yan kanal analizini, günümüzde polisin sıklıkla kullandığı, ilk kullanımı yine aynı yıllara rastlayan, kaçak esrar yetiştiriciliğini tespit etme yöntemi ile benzeştirebiliriz. 9 Aralık 1997'de ABD'nin Kolorado eyaletinde tarihin en büyük kaçak esrar yetiştiriciliği baskınlarından biri gerçekleştirildi. Polisin bu başarılı operasyonuna katkı sağlayan bilgiler, gizli olarak esrar yetiştirilen evin çatısının havadan termal sensör ile yapılan tarama sonucunda kırmızı görünmesi ve evin elektrik faturalarının çevresindekilere göre 10 kat fazla olmasıydı. Yani esrar yetiştiriciler yakalanmamak için gereken tüm güvenlik önlemlerini aldıkları halde, polisin yan kanallar yolu ile kendilerine ulaşmasına engel olamadılar. Her ne kadar bu örnekte yan kanal kullanımı iyi bir amaca hizmet etse de, kriptografik cihazların fiziksel işleyişleri farkında olunmadan kötü niyetli kişilerin gizli bilgilere ulaşmasına yol açabilir.

Yan kanal analizi, elektronik cihazların fiziksel özellikleri yoluyla, gizli tutulması gereken iç işleyişleri hakkında bilgi edinilmesidir. Mesela aşağıdaki grafik bir çarpma işlemine ait güç profilini gösteriyor. Çarpma işlemi süresince çarpılmakta olan anahtar sayı bit bit taranıyor ve bit değerlerine göre toplama ve ikiye katlama işlemleri yapılıyor. Anahtar sayının şu anki bit değeri 0 olduğunda sadece ikiye katlama işlemi yapılıyor, ama bu değer 1 olduğunda ikiye katlama ve toplama işlemleri art arda yapılıyor. Grafik üzerinde gösterildiği gibi, ikiye katlama işleminin toplama işlemine göre daha basit olması gerçeğinden yola çıkarak, tek başına ikiye katlama işlemi yapılan kesimleri ve ikiye katlama işlemini takiben toplama işlemi yapılan kesimleri ayırt edebiliriz. Bu da gizli tutulması gereken anahtar sayının kolaylıkla deşifre edilmesi demektir. Yan kanal güvenliği hiç göz önünde bulundurulmadan gerçekleştirilmiş bu algoritmanın güvenliği teoride ne kadar iyi olursa olsun, görüldüğü gibi pratikte algoritmanın işleyişi dışında hiçbir bilgiye ve uğraşa gerek duyulmadan kolaylıkla alt edilebilir. Aynı prensip günümüzde dünyada en yaygın olarak kullanılan açık anahtar kriptosunu kırmakta da kullanılabiliyor. Siz farkında olmasanız da, internette bir web tarayıcı ile alışveriş sitelerine girdiğiniz hemen hemen her sefer, güvenlik için bu algoritma kullanılıyor!



Güç ve zaman dışında başka fiziksel özellikler de, örneğin ses, elektromanyetik ışınım ve sıcaklık da yan kanal olarak kullanılabilir. Yan kanaldan pasif olarak yani sadece çalışmakta olan cihazı dinleyerek bilgi elde edilebileceği gibi, aktif olarak cihazı istenilen bir koşula yönlendirmek de mümkündür. Ayrıca yan kanal analiz teknikleri, bilginin işleniş yöntemi açısından da iki temel kola ayrılır. Yukarıdaki örnekte olduğu gibi bir veya birkaç ölçüm sonucu elde edilen bilgileri doğrudan yorumlayarak yapılan analizlere "basit yan kanal analizi" denir. Birbirleriyle korelasyon içeren birçok yan kanal ölçümünü istatistiksel olarak inceleyerek yapılan analizlere ise "diferansiyel yan kanal analizi" denir.

Günümüzde kriptografik cihazların algoritmik güvenliğinin yanı sıra yan kanal güvenliğine de büyük önem verilmektedir. Yan kanalları öngörmek ve yan kanaldan sızdırılan bilgi miktarını belirlemek kolay olmadığı için, yan kanal güvenliğini ölçmek veya mutlak güvenlikten bahsetmek de mümkün değildir. Yan kanal güvenliğinin öncelikli koşulu, yapılan farklı işlemlerin farklı fiziksel özellikler göstermesini engellemektir. Bu amaçla, cihaz-



Yan Kanallar

Basit oldukları için, koruyucu yüzeylerin ve devreye gömülü algılayıcıların kullanılması aktif yan kanal ataklarına karşı çekici bir çözüm alternatifi oluşturuyor. Fakat maalesef bu çözümler üretimde ciddi maliyet artışlarına sebep oluyor ve pratikte de çok rağbet görmüyor.

lar öncelikle basit yan kanal analizine karşı güvenli hale getirilmeye çalışılır. Yapılan çalışmalar, bilgiye bağlı olarak işlem seçimini engelleyerek yan kanaldan bilgi sızdırılmasını en aza indirmeye yöneliktir. Bu süreç, bilgiye bağlı olmaları durumunda performans artırmak amacıyla kullanılan hızlı algoritmalardan vazgeçilmesi ve daha yavaş olan ama bilgi sızdırmayan algoritmaların tercih edilmesi anlamına gelir. Örneğin bahsettiğimiz çarpma işlemini yan kanal açısından güvenli hale getirmek için öncelikle, anahtar sayının bit değerine bağlı olarak toplama işlemi yapılıp yapılmamasına karar verilmesini engellemeliyiz. Bu amaçla akla ilk gelen yöntem, anahtar sayının mevcut bit değeri 0 dahi olsa toplama yapmak ve sonucu göz ardı etmektir. Fakat, yalancı toplamalar diye adlandırılan bu yöntem de yeterince güvenli değildir. Aktif bir yan kanal analizcisi, sürmekte olan işleme yer yer hata iliştirip sonucun da hatalı olup olmadığını kontrol edebilir. Eğer sonuç da hatalıysa, yapılan toplama gerçek toplamadır ve anahtarın şu anki bit değeri gerçekten 1'dir. Eğer sonuç iliştirilen hataya rağmen doğruysa, yapılan toplama yalancı toplamadır ve anahtarın şu anki bit değeri 0'dır. Görüldüğü gibi yan kanallardan sızdırılan bilgiyi engellemek çok kolay bir iş değil. Öngörülen bir saldırıya karşı bilgi sızdırmayı engellemek için kullandığımız bir yöntem, sistemi öngöremediğimiz başka bir saldırıya karşı zayıf hale getirebilir. Örneğimizde verilen çarpma metodunu, yalancı işlemler içermeyen fakat yine de anahtar bitlerinden bağımsız olarak toplama ve ikiye katlama işlemi yapan algoritmalarla güvenli hale getirmemiz gerekir.

Yan kanal denildiğinde öncelikle akla ölçümü ve değerlendirmesi daha kolay olan "güç" ve "zaman" gelmektedir. Yukarıda verilen çarpma işlemi örneği, bu iki yan kanalın yapılmakta olan ara işlemleri nasıl ayırt edilebilir hale getirdiğini gösteriyor. Genellikle ihmal edilen fakat oldukça kuvvetli yan kanallardan biri de akustik kanalı, yani ses kanalıdır. Bir hesaplama esnasında işleme bağlı ses dalgaları da üretilir. Ses kanalı analizinin çok güzel bir örneğini Tromer vermiştir. Bu çalışmada önce standart bir bilgisayardaki işlemcinin çıkardığı ses, kriptografik bir algoritma çalıştırırken sıradan bir mikrofon ile kaydedilmiştir. Sonra bu ses, işlemcinin çalışma hızına göre parçalanıp işlemcinin komutları önceden teşhis edilen parmak izleri ile karşılaştırılarak, tek tek işletilen komutlar ortaya çıkarılabilmiştir.

Bir diğer yan kanal ise cihazların çalışırken yaydıkları elektromanyetik ışınımdır. Elektromanyetik ışınım tıpkı güç gibi yapılan işlemin ne kadar karmaşık olduğuna dair bilgi verebileceği gibi, daha detaylı bilgilere, örneğin bir hat boyunca akımın hangi yönde aktığı gibi bilgilere de ulaşmamızı sağlayabilir. 2001 yılında Karine Gandolfi ve çalışma arkadaşları farklı algoritmalar kullanan üç ayrı kriptografik cihaz üzerinde elektromanyetik analiz uygulamış ve her üç cihazın da gizli anahtarlarının tümünü elde etmeyi başarmışlardır. Çalışmakta olan bir kriptografik cihazın sıcaklığı da bize yapılmakta olan işlemin ne kadar güç harcadığı ve ne kadar



ısınmaya yol açtığı hakkında bilgi verir. Lokal sıcaklık değerlerinin çevreden izole edilerek ölçülmesi, diğer yan kanallarla karşılaştırıldığında daha çok emek isteyen bir iştir. Yine de ileri teknoloji ile üretilmiş termometreler sayesinde bu yan kanaldan da önemli bilgiler elde edilebilir.

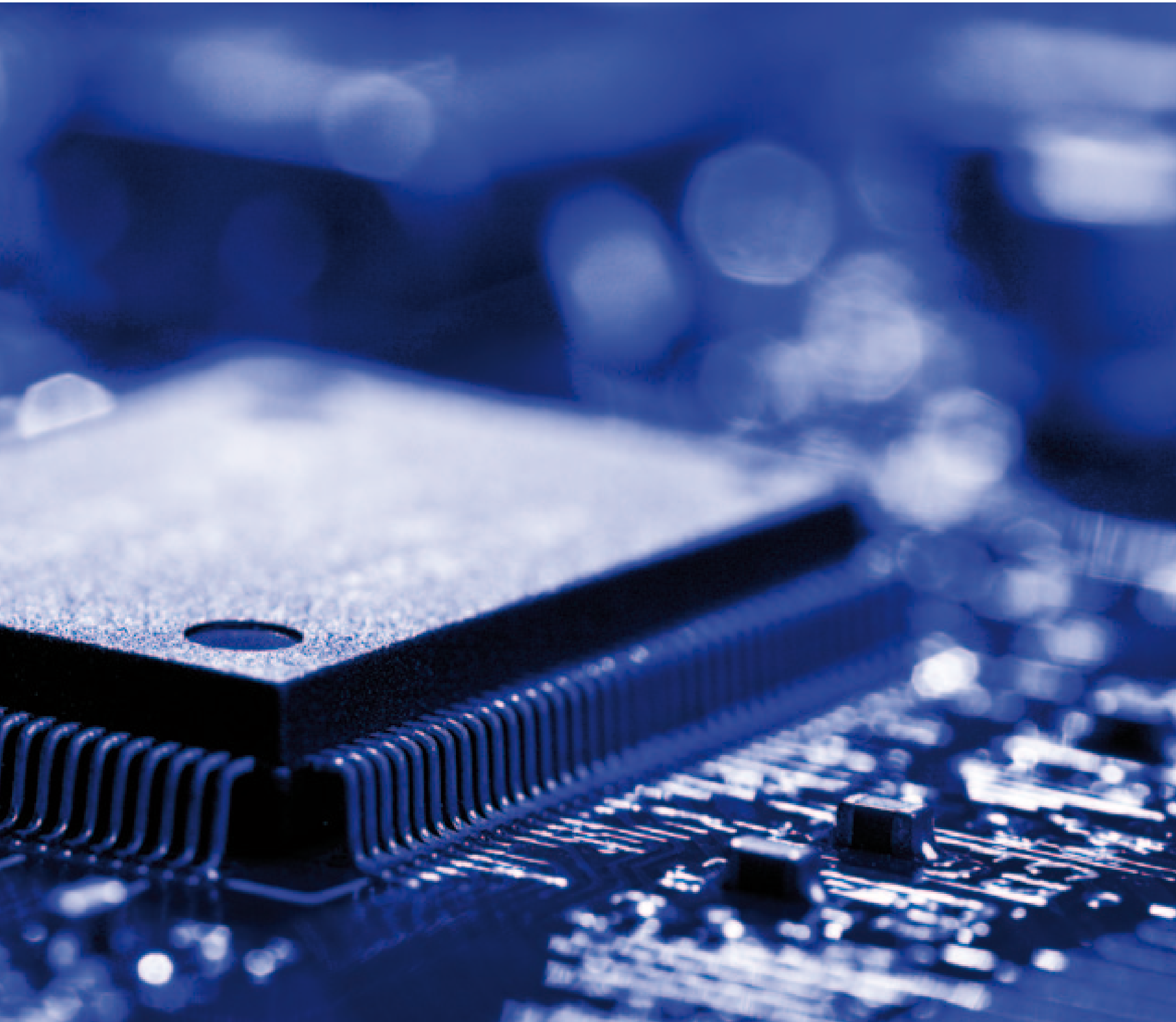
<<<

Tahmin edileceği üzere, daha gelişmiş donanım ile çok daha hassas yan kanal atakları gerçekleştirilebilir. Henüz birkaç yıl önce Skorobogatov'un gösterdiği gibi, bir çipin belleğinde kayıtlı bitleri tek tek okumak ve hatta değiştirmek mümkündür. Bu atağı gerçekleştirmek için yüksek çözünürlükte bir mikroskop, ucuz bir lazer ve biraz da el emeği yeterli olmaktadır.

Peki kripto cihazlarımızı bu kadar kuvvetli bir tehlikeye karşı nasıl koruyacağız? Bunun için önerilen çözümler kısaca şöyle özetlenebilir: Güç yan kanalını ortadan kaldırmak için, güç kullanımı dengelenmiş mantıksal kapılar kullanılabilir. Bu tür dijital devrelerde mantıksal kapılar işlenilen bit değerlerinden bağımsız ve hemen hemen sabit bir güç kullanır. Bu tür dijital tümleşik devre teknolojileri mükemmel olmasalar da kötü niyetli kişilerin işini hayli güçleştirir. Ayrıca dengeli bir güç dağılımı diğer yan kanalların da dengeli dağılmasını sağlayacaktır.

Basit oldukları için, koruyucu yüzeylerin ve devreye gömülü algılayıcıların kullanılması aktif yan kanal ataklarına karşı çekici bir çözüm alternatifi oluşturuyor. Fakat maalesef bu çözümler üretimde ciddi maliyet artışlarına sebep oluyor ve pratikte de çok rağbet görmüyor.

Yeni geliştirilen bir diğer çözüm de fiziksel olarak kopyalanması mümkün olmayan özelliklerin gizli bilgi saklamak için kullanılması. Bu tür devreler herhangi bir dış etki karşılığında sakladıkları bilgileri "kaybederler". Böylece bilgi sızması engellenmiş olur.



JUPITERIMAGES

Kaynaklar

Kocher, P., "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", *Uluslararası Kriptoloji Konferansı: Kriptolojide Gelişmeler (CRYPTO 1996),* Santa Barbara, Kaliforniya, ABD, Cilt 1109, s.104-113, 1996.

"Glowing Roof Leads Police to Marijuana: 263 Plants Confiscated from Area Warehouse", *The Gazette* gazetesi, Kolorado, ABD, 9 Aralık 1997.

http://people.csail.mit.edu/tromer/acoustic/

Gandolfi, K., Mourtel, C. ve Olivier F., "Electromagnetic Analysis: Concrete Results", *Kriptografik Donanım ve Tümleşik Sistemler Çalıştayı, (CHES 2001),* Paris, Fransa, Cilt 2162, s. 251-261, 2001.

Skorobogatov, S.P. ve Anderson, R.J., "Optical Fault Induction Attacks", *Kriptografik Donanım ve Tümleşik Sistemler Çalıştayı, (CHES 2002),* Redwood Shores, Kaliforniya, ABD, Cilt 2523, s. 2-12, 2002.

Tekin Dereli

Prof. Dr., Fizik Bölümü
Koç Üniversitesi

İletişimde Mutlak Güvenlik İçin Kuantum Kriptografi

Kuantum kriptografi konusu alışılmadık kuantum teknolojilerine iyi bir örnektir. Bir foton çiftinin dolaşık bir kuantum durumunda hazırlandığını düşünelim. Bu dolaşık çifti özel optik lifler üzerinden uzayda birbirlerinden -aralarındaki mesafe çok uzun olacak şekilde- ayırır ve bizde kalan fotonun kutuplanma yönünü ölçerek belirlersek, eş-anlı olarak iyice uzakta olan ötekinin kutuplanma yönünü de belirlemiş oluruz. Bu çok hassas deney ilk kez 1997'de yapılabildi. Bugün artık piyasada, dolaşık foton çiftleri üstüne kurgulu "kuantum teleportasyon" yöntemiyle, birkaç yüz kilometrelik mesafe aralıklarında bile yüzde yüz güvenlikli kuantum anahtar dağıtımı yapılıyor.

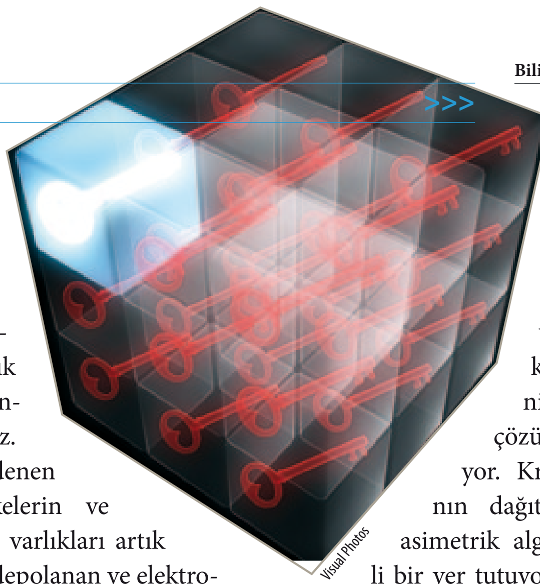


Prof. Dr. Tekin Dereli Koç Üniversitesi Fizik Bölümü öğretim üyesidir. Yüksek lisans ve doktora derecelerini ODTÜ Fizik Bölümü'nde aldıktan sonra ABD ve Avrupa'nın tanınmış üniversitelerinde araştırmacı ve misafir profesör olarak bulunmuştur.
Uzun yıllardır üniversitelerimizde ileri düzeyde dersler vermekte ve doktora öğrencileri yetiştirmektedir. Kuantum mekaniği, kuantumlu ayar alanları ve genelleştirilmiş gravitasyon teorileri üstüne yayımlanmış 100'den fazla makalesi bulunmaktadır. 1996 TÜBİTAK Bilim Ödülü'nü kazanmıştır. Halen TÜBA Konseyi üyesidir. Prof. Dr. Tekin Dereli 1993-2000 yılları arasında TÜBİTAK *Bilim ve Teknik* dergisinde Yayın Kurulu üyesi olarak görevliydi.

Tarihsel gelişimine bakarsak kuantum mekaniği, gazların ışıma ve soğurma spektrumlarının neden her atomun kendisine özgü kesikli çizgilerden oluştuğunu açıklamaya çalışırken keşfedilmiştir. 1900 yılı Aralık ayında Alman fizikçi Max Planck'ın enerji kuantumları varsayımıyla başlayan kuantum serüvenindeki en önemli aşamalardan birisi, Albert Einstein'ın "foton" adı verilen ışık kuantumları yardımıyla fotoelektrik etkiyi açıklayabilmesi olmuştur. Einstein 1921 Nobel Fizik Ödülü'nü özel görelilik teorisi ile değil bu buluşu nedeniyle -hidrojen atomu modelini kuran Niels Bohr ile birlikte- 1922 yılında aldı. Bohr'un atomun kuantum teorisine Werner Heisenberg, Erwin Schrödinger ve Paul Dirac tarafından son halinin verilişini, yani kuantum mekaniğinin keşfini 1925-1930 arası diye kabul edebiliriz. Gerçi günümüzde atom çekirdeklerini oluşturan proton ve nötronların iç yapısını araştırma noktasını bile geçtik, ama genelde kuantum mekaniğini anlatırken 1930'larda yapılan buluşların ötesine pek geçilemiyor. Çünkü kuantum fiziğinde klasik fiziktekinden çok farklı bir dil ve alışılmadık, yep-

yeni kavramlar kullanılır. Kuantum mekaniğini anlıyorum demek ve doğru anlatabilmek hiç kolay değil. 1930'ların Kuantum Devrimi'nin gündelik yaşamımıza en çarpıcı yansımaları kanımca 1940'lardan sonra nükleer enerji üretiminin ve kullanımının yaygınlaşması, 1950'lerde transistorların devrelerde kullanılmasıyla başlayan mikroelektronik uygulamalar ve 1960'lardan sonra lazerlerin bulunması ve bunlara dayalı yeni iletişim teknolojilerinin geliştirilmesidir. Kuantum mekaniğinin gelişimi günümüzde de durmuş değil, hiç beklenmedik sürpriz buluşlar ve uygulamalarla 21.yüzyılda da sürüyor.

Kuantum etkilerinin yerel olmaması, teorinin keşfedildiği ilk günlerden başlayarak büyük tartışmalara neden oldu. Albert Einstein 1935'de "EPR paradoksu" diye adlandırılan bir düşünce deneyi üzerinde duruyor, kuantum etkilerinin fiziğin en temel varsayımlarından biri olan göreli neden-sonuç ilişkilerini bozacağını düşünüyordu. Yani kuantum etkileri yoluyla ışıktan hızlı bilgi iletiminin yapılabilirliği söz konusuydu. Einstein, bu mümkün olamayacağına göre kuantum mekaniğinin temelinde tutarsızlık olduğunu iddia ediyordu. Kuantum mekaniğinin felsefi temelinin oluşumuna büyük katkıları bulunan Niels Bohr Einstein'ın bu iddialarını anında yanıtladı. Ancak 1980'lere gelene dek Bohr'un savunduğu kuantum mekaniği yorumunun mu, yoksa Einstein'ın iddiasının mı haklı olduğunu kanıtlayacak herhangi bir gözlemsel veri yoktu. Teknolojinin ilerlemesiyle olanaklı hale gelen ve 1982'de yapılan deneyler kuantum mekaniğinin yerel olamayacağını, yani Einstein'ın haklı olmadığını artık göstermiştir. Bu olgunun klasik fizik kavramlarından ne denli farklı düştüğü, popüler düzeyde "Schrödinger'in kedisi" denen bir düşünce deneyi ile anlatılmak istenir. Kuantum mekaniğinin yerel olmaması ve buna benzer alışılmadık niteliklerinin ciddiye alınması ve bunlara uygulama aranması için bir 10 yıl daha geçti. Bu anlamda 1995 çok keskin bir dönüm yılıdır. Ayrıntılarına burada giremeyeceğim pek çok nedenden dolayı kuantum iletişim ve bilişim teknolojileri ile nanoteknolojinin başlangıcı olarak algılanan 1995 yılına 2. Kuantum Devrimi deniyor. 21.yüzyılla beraber artık kuantum mühendisliği çağındayız.



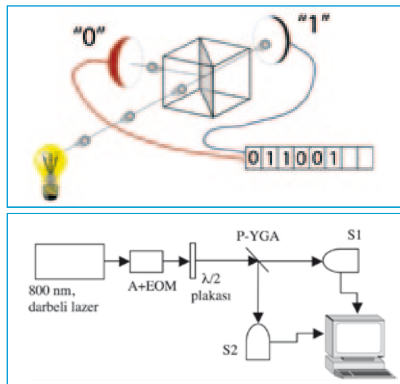
Bilgi çağı denen çağımızda, ülkelerin ve kişilerin değerli varlıkları artık bilgisayarlarda depolanan ve elektronik ağlarda taşınan verilerden ibaret. Bu tip verilere banka hesapları, devletin, sanayi ve ticaret kuruluşlarının gizli bilgileri gibi pek çok farklı örnekler verilebilir. Kişiler ve kurumlar arasında aktarılan bu bilgilerin gizliliğini sağlamak, değiştirilmesini engellemek, kaynağından emin olmak gibi temel güvenlik servisleri, kriptoloji biliminin matematiksel çözümleriyle sağlanıyor. Kripto anahtarlarının dağıtımında özellikle asimetrik algoritmalar önemli bir yer tutuyor. Ancak son yıllarda 5-6 bitlik kuantum bilgisayarlarının yapılabilirliğinin gösterilmiş olması, bu bilgisayarların büyük ölçekte gerçeklenmesiyle, kriptolojide önemli bir yer tutan günümüzün asimetrik algoritmalarını kırılabilir hale getirecektir. Bu,

Kuantum Fiziksel Rastgele Sayı Üreteci

Kuantum fiziksel rastgele sayı üretimi, kuantum fiziğinin ölçüm aksiyomunun bir sonucu olarak ortaya çıkar. Ölçüm aksiyomuna göre yarı geçirgen bir aynanın girişine tek fotonlar gönderildiğinde, geçirme ve yansıma çıkışlarındaki iki algılayıcıdan yalnızca biri eş-anlı algılama yapacaktır. Dolayısıyla yarı geçirgen aynanın çıkışındaki iki algılayıcıda yapılan algılamalar 0 ve 1 ile kodlandığında, yapılan algılamaların serisi ideal bir rastgele sayı üretecektir.

Kuantum fiziksel rastgele sayı gösterimi için kullanılması planlanan deneysel altyapı Şekil 1'de gösterilmektedir. Bir darbeli lazerin ışıma gücü yüksek oranda düşürülerek darbe başına 0,05 foton üretilen merteबeye getirilir. Bir λ/2 plakası ile gücü düşürülmüş lazer ışımasının doğrusal polarizasyonu 45° döndürülür. Polarize yarı geçirgen ayna (P-YGA) kullanılarak λ/2 plakasının çıkışındaki lazer ışımasının geçiren ve yansıtan kollara ayrılması sağlanır. Lazerin gücünün çok düşürüldüğü limitte, P-YGA'nın iki çıkışında bulunan tek foton sayaçlarından en fazla biri darbe başına foton algılayacaktır. Bu algılayıcıların algılamaları 0 ve 1 ile kodlanarak elde edilen bit serisi ile rastgele sayı üretimi gerçekleştirilmiş olacaktır.

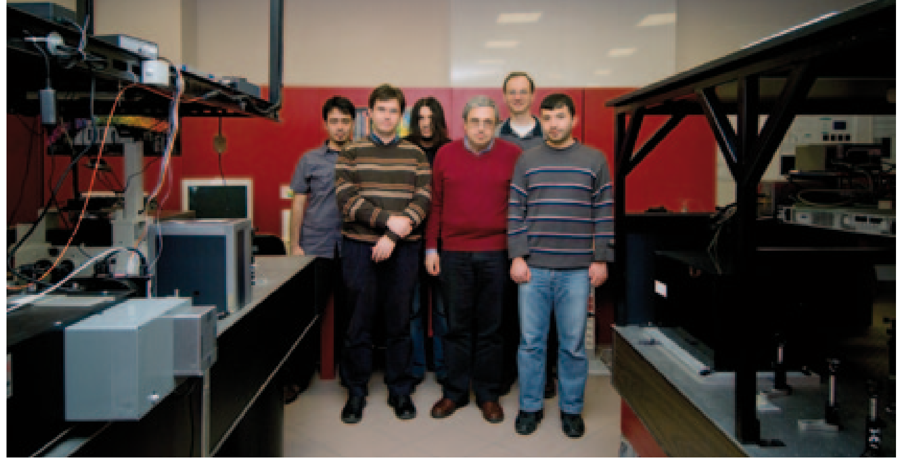
Tek foton kaynaklarının temininden sonra kuantum kriptoloji sistemlerinin performansı büyük ölçüde tek fotonları bile algılayabilen tek foton sayaçlarının performansına bağlıdır. Tek foton sayaçları fotonları elektronlara çeviren aygıtlardan, hızlı güçlendirici devrelerden ve oluşan sinyalleri ölçebilen devrelerden oluşur. Günümüzde avalanş-fotodiyotlar, fotoğüçlendiriciler (*photo-multipliers*), çok kanallı levha (*multichannel plate*) ve süperiletken Josephson eklemli (*Josephson junction*) aygıtlar, fotonları yüksek kuantum verimlilikle elektronlara çevirir.



Kuantum fiziksel rastgele sayı üreteci için kullanılması öngörülen deneysel düzenek. A, lazer güç düşürücü filtreler; EOM, Elektro-optik modülatör; P-YGA, Polarize yarı geçirgen ayna; S1, S2 tek foton sayacı

kriptolojinin temel güvenlik unsuru olan kripto anahtarlarının güvenli dağıtımına yönelik büyük bir tehdittir. Kuantum anahtar dağıtımı bu tehdide karşı öne sürülmüş pratik bir çözümdür. Halihazırda büyük ölçekli kuantum bilgisayarı henüz gerçeklenememiş olmasına rağmen, başarılı kuantum anahtar dağıtım sistemlerinin çalışan örnekleri verilmiştir. Gizli bilgilerin başarıyla korunmasının bir ülkenin ekonomik ve sosyal yaşamındaki önemi aşikârdır. Günümüzde özellikle gelişmiş devletler birbirlerinin sırlarını öğrenmek için yüksek teknolojiye dayalı dinleme ağları ve kripto analiz altyapıları oluşturmuştur. İleri devletler bu aşamalardan da ileri giderek kuantum kriptolojiye bankacılık gibi özel sektör uygulamalarında da yer verir olmuşlardır.

Günümüzün kritik teknolojileri arasında bulunan kuantum kriptoloji konusunda uluslararası düzeyde çalışmaların yürütüldüğü birçok araştırma merkezi vardır. Bu konuda lider şirketler (merkezi Boston'da olan BBN, New York'ta olan MagiQ ve Cenevre'de olan idQuantique) çeşitli bankalar ve finans kuruluşları için kuantum kriptoloji cihaz ve yazılımları sunmaktadır. Her ne kadar çeşitli askeri kuruluşların ve gizli servislerin de kuantum kriptolojiden istifade ettiği düşünülse bile, gizlilik kuralları nedeniyle bu konuda geçer veri elde etmek olanaksızdır. Bilinen tek açık hükümet uygulaması, İsviçre'de 2007 Cenevre Kanton seçimlerinde kâğıt oyların girildiği bilgisayarlar ile tüm oylarla ilgili verilerin toplandığı merkez arasındaki bilgi transferinin emniyeti için kuantum kriptoloji kullanılmasıdır. Dünyada pek çok ülke kendi kuantum bilgi teknolojileri ve özellikle kriptoloji merkezlerini kurmuş ve kurmakta. Avrupa'daki tüm ülkelerin, uzak doğuda Singapur ve Tayland dahil tüm ülkelerin, Güney ve Kuzey Amerika ülkelerinin ve Avustralya'nın kuantum teknolojileri konusunda uzmanlaşmış merkezleri vardır. Bu merkezler üniversite bünyesinde veya

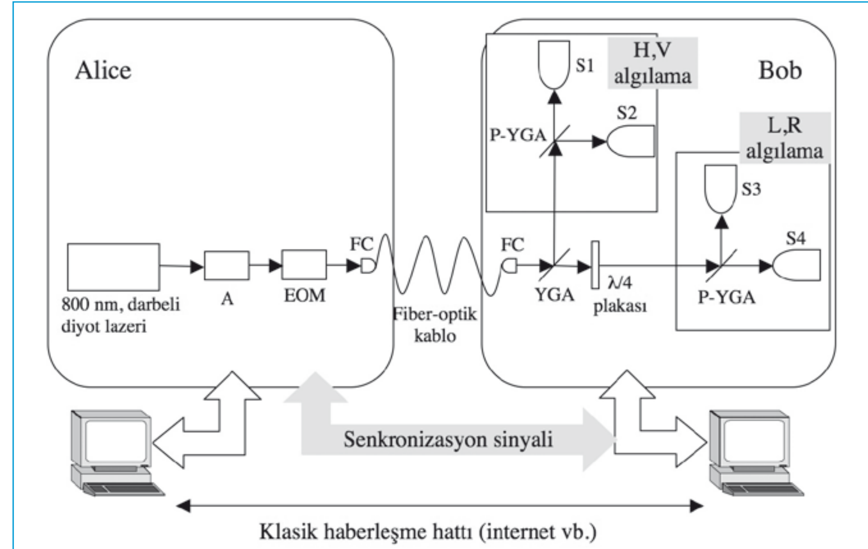


Prof. Dr. Tekin Dereli ve proje ekibi Koç Üniversitesi'ndeki laboratuvarlarında

Kuantum Anahtar Dağıtımı

Tek fotonlar kullanılarak kurulan bir haberleşme hattında ideal güvenlikte bilgi alışverişi gerçekleştirmek de mümkün. Böyle bir haberleşme hattında, dinleme yapan bir casusun kaydedeceği bilgiler göndericiden alıcıya ulaşamaz. Dolayısıyla alıcı için bir bilgi değeri taşımaz. Öte yandan alıcı tarafına bir bilgi ulaştığında, bu bilginin bir casus tarafından dinlenmemiş olduğu da kesin olur. Bu özellik kullanılarak, kriptoloji sistemlerinde ideal güvenlikte anahtar dağıtımı gerçekleştirilebilir. Tek fotonlar kullanılarak yapılan bu anahtar dağıtımına "kuantum anahtar dağıtımı" denir.

Kuantum anahtar dağıtımı için kurulması planlanan deneysel düzenek Şekil 2'de gösterilmektedir. Işık kaynağı olarak, kuantum fiziksel rastgele sayı üreteci uygulamasında da kullanılması öngörülen, 40-50 MHz'lik oranlarda 1 nanosaniyeden düşük zaman uzunluğuna sahip darbeler üretebilen bir lazer kullanılır. Darbeli lazerin gücü düşürülerek darbe başına ortalama olarak çok düşük sayıda (<~ 0.05) foton üretilen limite ulaşılır. Lazerden çıkan fotonlar hızlı bir elektro-optik modülatör kullanılarak doğrusal ya da çembersel tabanda polarizasyonlara kodlanır. Bob tarafında fotonlar bir yarı geçirgen ayna, polarize yarı geçirgen aynalar ve bir λ /4 plakası yardımı ile dik ya da çembersel tabanda algılanır.



Kuantum anahtar dağıtımı için kullanılması öngörülen deneysel düzenek. A, lazer güç düşürücü filtreler; YGA, Yarı geçirgen ayna; P-YGA, Polarize yarı geçirgen ayna; EOM, Elektro-optik modülatör; S1, S2, S3, S4, tek foton sayaçları; FC, fiber uyarıcı

ulusal ya da ticari Ar-Ge kuruluşları bünyesinde oluşmuştur. Nihai proje ancak bu merkezler arasındaki ortak çalışmaların yaratacağı sinerji ile başarıya ulaşmaktadır. Örneğin askeri amaçlı kuantum teknolojileri ulusal merkezlerin ve üniversite merkezlerinin ortak çalışması ile gerçekleştirilirken, bankalar için yapılan bir projede şirketler ve üniversiteler beraber çalışmıştır. Başarılı bir örnek olarak Toshiba ve Fujitsu gibi şirketlerin kuantum teknoloji merkezlerinin, Tokyo Üniversitesi kuantum bilişim gruplarıyla ortak çalışmaları verilebilir. IBM, NEC, Fujitsu, Toshiba gibi birçok şirketin yanı sıra hükümetler de özellikle kuantum bilgi teknolojileri konusuna öncelik vermektedir. Bu nedenle rekabet halindeki şirketler bile ortak merkezler kurmuştur. Mitsubishi ile NEC, Tokyo Üniversitesi ile ortak bir merkez kurmuştur. Avrupa Birliği, Amerika'nın elindeki Echolon sistemi sebebiyle endişe duymakta ve buna cevaben kuantum teknolojilerini kullanmak niyetini dile getirmektedir. Bu sebeple, çerçeve programları gibi destek programlarında kuantum haberleşme öncelikli konulardandır. Japonya ve Çin bilim bakanlıkları da kuantum teknolojilerini öncelikli alanları arasına almıştır. Çin 2007 de ilk başarılı kuantum iletişim ağını Pekin-Tianjin arasında operasyonel hale getirdiğini açıklamış ve Çin Network Şirketi bünyesinde ticari kılındığını duyurmuştur. Amerika da bu rekabet karşısında DARPA önderliğinde kuantum teknolojilerine ayırdığı kaynakları artırmıştır. BBN şirketine sadece 2008 yılında 3,5 milyon dolar yardım yapılmıştır. Bu şirket, hükümetten aldığı toplam 15 milyon dolar destekle üniversiteler ve ulusal araştırma merkezleri ile beraber kuantum kriptoloji ve kuantum haberleşme konularında yoğun faaliyet göstermektedir. Amerikan Ulusal Ölçüm Merkezi (NIST) gibi kuruluşlar da uzun mesafeli kuantum haberleşme ağlarına yönelmiştir.

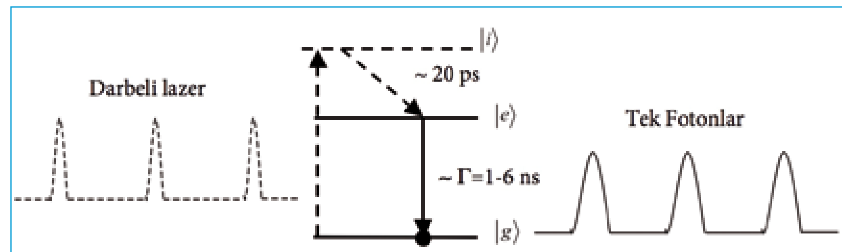
Türkiye'nin ilk "state-of-the-art" (günün gereklerine uygun) kuantum teknolojileri araştırma laboratuvarlarından biri, bu sene başında Devlet Planlama Teşkilatı'nca 3 yıl desteklenmesi kabul edilen bir altyapı projesiyle Koç Üniversitesi'nde kurulacaktır. Projede görev alan Prof. Dr. Tekin Dereli, Doç. Dr. Özgür Müstecaplıoğlu ve Doç. Dr. Alper Kiraz kuantum fiziğinde uzman, ülkemizde ve yurt dışında tanınan öğretim üyeleridir. Yüksek lisans öğrencileri Yasin Karadağ, Ramazan Uzel ve Utkan Güngördü proje çalışmaları kapsamında tezlerini hazırlamaktadır. Bu laboratuvarda ve buna paralel olarak TÜBİTAK UEKAE bünyesinde kurulmakta olan Kuantum Teknolojileri Araştırma Laboratuvarları'nda yapılacak ortak çalışmalar ile ülkemizin ilk kuantum kriptografi sistemi geliştirilecek ve kuantum bilişim konusunda ülkemizde gelecekte yapılacak çalışmalara öncülük edecek bilgi birikimi, altyapı ve sinerji oluşturulmuş olacaktır.

Günümüzde kuantum kriptografi ağırlıklı kripto anahtar dağıtım sistemleri iki ortamda gerçeklenmektedir: Fiber op-

Tek Foton Kaynağı Gösterimi

Tetiklemeli tek foton kaynakları ideal olarak bir tetikleme sonucu bir ve yalnız bir foton yayan aygıtlardır. Pratikte foton toplama verimliliğinden kaynaklanan sınırlamalar ile her tetikleme sonucu yayılan foton toplanamasa da, bu aygıtlar ile her tetikleme sonucu bir ya da 0 foton yayılımı sağlanabilmektedir. Tetiklemeli tek foton kaynakları, iki seviyeli sistemin darbeli lazer ile uyarılmasıyla elde edilir. Şekil 3'te gösterildiği gibi bu uyarım yönteminde lazerin dalgaboyunu, yayılan tek fotonların dalgaboyundan farklı tutmak için üçüncü bir enerji seviyesi sıkça kullanılır. Darbeli lazerin her bir darbesi, iki seviyeli sistemin bir defa uyarılmış (|i>) seviyeye geçişine neden olur. Bu sistem daha sonra |e> seviyesine hızlı bir şekilde geçer ve |e> ile |g> seviyeleri arasındaki geçişte kendiliğinden ışıma ile tek bir foton yayar. Bu şekilde, her bir darbenin tek bir foton ışımasını tetiklemesi sağlanabilir. Her bir darbenin tek bir foton ışımasını tetiklemesi için, darbe zaman aralığının kendiliğinden (spontane) ışıma zamanından yeterince küçük olması ve darbe enerjisinin de iki seviyeli sistemi, uyarılmış enerji seviyesi olan |i>'ye çıkaracak kadar yüksek olması gerekir. Bu tür deneysel gösterimlerde şu ana kadar iki seviyeli sistem olarak tek boya molekülleri, tek InAs kuantum noktaları, tek CdSe kuantum noktaları, tek atomlar, elmas içindeki N (azot) - boşluk merkezleri veya tek karbon nanotüpleri kullanılarak, oda sıcaklığında veya sıvı Helyum sıcaklıklarında gösterimler gerçekleştirilmiştir. Proje kapsamında, uygun bir iki seviyeli sistem seçilerek tetiklemeli tek foton kaynağı gösterimi gerçekleştirilecektir.

Kullanılacak deney düzeneği Şekil 4'te gösterilmektedir. Bu düzenekte düşük yoğunlukta iki seviyeli sistemler içeren örnek, sıvı Helyum soğutucusunda (cryostat) korunur. Darbeli lazer ile örnek üzerinde optik çözünürlükle belirli bir alan (~1 mm^2) uyarılır. Bu alanda bulunan tek bir iki seviyeli sistem uyarılır ve toplanan ışıma çizgisi bir bant geçiren girişim filtresi kullanılarak Hanbury Brown ve Twiss deney düzeneğine gönderilir. Bu düzenekte rastgele algılama elektronik aygıtları kullanılarak ışımanın ikinci derece faz uyumu fonksiyonu ölçülür. İkinci derece faz uyumu fonksiyonunun ölçülmesi ile tetiklemeli tek foton ışıması gösterimi gerçekleştirilir.



Tetiklemeli tek foton kaynağının çalışma prensibi.

tik hat üzerinden haberleşen sistemler ve havadan (*free space*) haberleşen sistemler. Her iki sistem için de şimdiye kadar uygulanmış veya uygulanması planlanan dört farklı yaklaşım vardır: 1) Zayıflatılmış lazer kaynakları kullanan sistemler: Bu yaklaşımda lazerler tarafından üretilen zayıflatılmış ışık darbeleri fiber veya hava yoluyla karşı tarafa iletilir. Fiber üzerinden zayıflatılmış lazer kaynakları kullanan sistemler, tek mod fiber üzerinden çalışırlar ve 1330 nm veya 1550 nm dalgaboyu civarında çalışırlar. Hava üzerinden zayıflatılmış lazer kaynakları kullanan sistemler ise atmosferik optik haberleşme sistemlerinden yararlanır. 2) Tek foton kaynağı kullanan sistemler, her seferinde tek foton ürettikleri için bilgi sızıntısı ihtimalini ortadan kaldırır. 3) Dolaşık (*entangled*) foton kaynağı kullanan sistemlerde ise iki kuantum sistemi arasındaki yerel olmayan (*non-local*) kuantum mekaniksel etkilerden yararlanılır. Bu yerel olmayan etkiler, anahtar değişimi için kullanılabilmektedir. 4) Sürekli değişken (*continuous variable*) kullanan sistemlerde anahtar, kuvvetli optik darbelerin fazlarındaki, genliklerindeki veya kutuplanmalarındaki küçük sapmalarla kodlanır. Bu kodlama ikili veya sürekli ta-

Zafer Gedik

Mühendislik ve Doğa Bilimleri Fakültesi, Sabancı Üniversitesi

Kuantum Bilgisayarları

Tek bir bilgisayar yerine her biri farklı bir evrende, aynı anda çalışan birçok bilgisayar kullanarak işlemleri çok daha hızlı yapabilir miyiz? Dünyadaki tüm bilgisayarları kullansak bile, evrenin yaşından daha fazla zaman gerektirecek hesaplamaları kısa sürede tamamlayabilir miyiz? Kuantum bilgisayarları sayesinde her iki soruya da olumlu cevap verebiliriz. Üstelik bu aygıtların ilkel örneklerine bakılırsa kuantum bilgisayarlarının kullanıma girmeleri çok uzak görünmüyor.

Kuantum bilgisayarlarının klasik bilgisayarlarla çözülemeyen hangi problemleri verimli bir şekilde çözebilecekleri tümüyle anlaşılmış olmasa da kesin olarak bildiğimiz, sadece onlara has bir üstünlüklerinin olduğudur: Rastgele sayılar üretmek. Belirlenimci yapıları nedeniyle klasik bilgisayarlarla elde edilen sayılar hiçbir zaman tam rastgele sayılar olamamaktadır. Kuantum mekaniğinin temel ilkeleri arasında yer alan rastgelelik, aynı özelliğe sahip sayılar elde etmek için doğal bir kaynak oluşturur.

Kuantum bilgisayarını klasik bir bilgisayardan ayıran nedir? Doyurucu olmasa da kısa bir cevap şöyle verilebilir: Aygıt, klasik fizik yerine kuantum fiziğinin ilkelerine göre çalışmaktadır. Bilgisayarları bizim seçtiğimiz bir ilk halden başlayıp son hale giden birer makine olarak düşünebiliriz. Son hal aslında istediğimiz cevabı ya da bilgiyi taşıyan bir durumdur. İşte bu iki hal arasında sistemin nasıl devineceği birtakım fizik kurallarınca belirlenir. Örneğin mevcut birçok bilgisayarda olduğu gibi klasik elektronik devre denklemleri bu kuralları belirleyebilir. Sadece giriş ve çıkışlara bakarsak, hepsinde ikilik tabanın elemanları olan 0 ve 1'lerden başka bir şey görmeyeceğimiz için farkı anlayamayabiliriz. Fark, bilgisayarda çalıştırabileceğimiz algoritmalarda görülebilir. Ayrıca kuantum algoritmaları çoğu kez bir başarı olasılığıyla birlikte verilirler, yani bilgisayarın istediğimiz cevabı bulamama olasılığı da vardır. Bu durumda başa dönüp tekrar hesap yapmamız gerekir.

Kuantum mekaniğinin bilim felsefesine getirdiği yeniliklerden biri de gözlemcinin ya da yapılan gözlemin yorumlanmasının tartışmaya açık olmasıdır. Çok sayıda evren ya da paralel evrenler modeli konuyla ilgili fikirlerden biridir. Kuantum bilgisayarları için paralel evrenler fikrini her tür bilgiyi yazmada kullanabileceğimiz 0 ve 1'lerle açıklayabiliriz. Klasik bilgisayarlarda 0 ve 1 değerlerini bit adını verdiğimiz birimlere kaydederiz. Kuantum bilgisayarındaysa kuantum bitleri ya da kısaca kubitler bulunmaktadır. Giriş ve çıkışta sadece 0 ve 1'leri görsek de kuantum bilgisayarının ara hallerini betimlerken kubitlerin hem 0 hem de 1 oldukları haller de varmış gibi görünür. Kuantum bilgisayarlarını klasik bilgisayarlardan ayıran belki de en önemli özellik işte bu üst üste binme (0 ve 1'in üst üste binmesi) halleridir. "Olur mu öyle şey? Ya 0 ya 1'dir!" diye ısrar eder ve değerinin ne olduğunu gözlemeye kalkarsak bu ara hallerde, başlangıç şartları aynı olmasına rağmen, bazen 0 bazen 1 görürüz. Kopenhag yorumlaması adı verilen yaklaşımda deneyin her tekrarında sadece olasılıkların bilinebileceği düşünülür. Paralel evrenler yorumlaması ise bu olasılık tabanlı, bir anlamda her şeyin rastgelelik üzerine kurulduğu yaklaşım yerine 0 ve 1'in ikisinin de ama farklı evrenlerde gözlendiği fikri üzerine inşa edilmiştir.

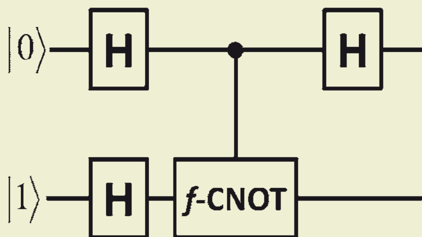
Üst üste binme hallerini matematiksel olarak $p|0\rangle+q|1\rangle$ şeklinde gösteriyoruz. Kubitlerin $|0\rangle$ ya da $|1\rangle$ şeklinde yazılması kuantum mekaniğinde Dirac tarafından geliştirilmiş bir gösterim şeklidir. Bu kubit değeri neymiş diye bakmaya kalkarsak p^2 olasılıkla 0, q^2 olasılıkla 1 görürüz. Buradan, $p^2+q^2=1$ olması gerektiğini tahmin etmek zor değildir. Aslında p ve q karmaşık (kompleks) sayılar da olabilir ama biz şimdilik kendimizi gerçek sayılarla sınırlayalım. Hatta $p^2=q^2=1/2$ olduğu durumlar basit bir kuantum algoritmasını anlamamıza yeterli olacaktır. Giriş sadece 0 ya da 1 olabiliyorsa klasik bir kubit için mümkün olmayan, örneğin $|0\rangle+|1\rangle/\sqrt{2}$ ya da $|0\rangle-|1\rangle/\sqrt{2}$ gibi halleri nasıl elde edebiliriz? İşte kuantum mekaniksel davranış burada işin içine girer. Klasik bilgisayarlardaki gibi burada da kapılar (kubitlerin hallerini değiştiren birimler) inşa etmek mümkündür. Örneğin, ışık tanecikleri fotonlar için laboratuvarda gerçekleştirmesi çok kolay olan Hadamard kapısı bunlardan biridir. Hadamard kapısı girişine $|0\rangle$ uygulandığında $|0\rangle+|1\rangle/\sqrt{2}$, $|1\rangle$ uygulandığındaysa $|0\rangle-|1\rangle/\sqrt{2}$ verir. Kapıları kontrollü olarak uygulamak da mümkündür. Örneğin, bir kubit değil işlemini (0'ı 1, 1'i 0 yapma) başka bir kubitin "0 duru-

banlardan birinde olabilir. Proje çalışmalarının başlangıç aşamasında, tek-modlu optik fiber üzerinden zayıflatılmış lazer kaynakları kullanan bir sistem geliştirilecektir.

Eğer Koç Üniversitesi ve UEKAE birlikte yukarıda bahsi geçen kuantum kriptoloji altyapısını ve teknik gelişimini sağlayabilirlerse, ülkemiz gelişmelerden geri kalmayarak bu sahada da söz sahibi olacaktır. Kurulacak bu laboratuvarlar ile, ideal güvenilirlikte haberleşme hatları ve mevcut klasik bilgisayarlardan çok daha hızlı çalışabilen bilgisayarlar vaad eden bu önemli alanda Türkiye'de ilk defa rekabetçi bir güç oluşturulması hedeflenmektedir. Bu altyapı sayesinde RSA (Rivest, Shamir, Adleman) kripto-sistemi gibi birçok algoritmaya karşı ve halihazırda ülkemizde kullanılan E-imza, internet bankacılık, internet alışverişi gibi sistemlere yönelik olası tehdit oluşturan kuantum hesaplamalara dayanıklı, yeni algoritmaların tasarlanması imkânı doğacaktır. Kuantum kriptografi sahasında kazanılan bilgi birikiminin kuantum hesaplama alanına doğru gelişmesine olanak sağlanacak, böylece birçok yeni uygulama için de bilgi birikiminin yolu açılmış olacaktır.

munda uygula, 1 olması durumunda uygulama," demek mümkündür. Önemi ve yaygınlığı nedeniyle bu işleme bir isim verme gereği görülmüş, kontrollü değilleme adı verilmiştir. Hadamard kapısını kısaca H, kontrollü değilleme kapısını da kısaca CNOT ile göstereceğiz. İşi biraz daha karıştırıp f - CNOT kapısını tanımlayabiliriz ki, $|x\rangle|y\rangle \xrightarrow{f\text{-CNOT}} |x\rangle|y \oplus f(x)\rangle$ şeklinde tanımlanan bu kapı $f(x)= x$ durumunda CNOT'a indirgenir. Burada $\oplus$ işlemi modüler toplamı göstermektedir (mod 2). Yani $0 \oplus 1 = 1 \oplus 0 = 1$ ve $0 \oplus 0 = 1 \oplus 1 = 0$'dır.

Kuantum algoritmaları bir problemi nasıl hızlı çözebilmektedirler? Basit bir benzetme yaparsak, örneğin, iki çubuğun boylarını karşılaştırıp hangisinin daha uzun olduğunu anlamaya çalıştığımızı düşünelim. Bir yöntem, iki çubuğun da boylarını ölçüp sonuçları karşılaştırmaktır. Diğer bir yöntemse iki çubuğu yan yana koyup doğrudan hangisinin daha uzun olduğunu görmektir. Klasik bilgisayarın ilkini, kuantum bilgisayarının da ikincisini yaptığını düşünebiliriz. Bu benzetmeyi daha açık bir hale getirmek için ilk kuantum algoritmamız olan Deutsch algoritmasından bahsetmek yerinde olacaktır. H ve CNOT kapıları bu algoritmayı uygulamak için yeterlidir. Amacımız bir fonksiyonun 0 ve 1 için değerlerinin aynı olup olmadığını anlamak olsun. Yani $f(0) = f(1)$ mi yoksa $f(0) \neq f(1)$ mi? Tıpkı çubuk boylarını karşılaştırma probleminde olduğu gibi $f(0)$ ve $f(1)$'i hesaplayarak, yani iki işlem yaparak bu soruya cevap verebiliriz. Ancak bunu kuantum bilgisayarı, daha doğrusu basit bir kuantum işlemcisi kullanarak tek hesapla yapmak mümkündür. Yani f fonksiyonunu yalnız bir kez hesaplayarak 0 ve 1'de aynı değeri alıp almadığını tespit edebiliriz. Bunun için gereken, aşağıdaki kuantum devresi'dir.



Kuantum işlemcisi Deutsch algoritması yardımıyla fonksiyonu yalnız bir kez hesaplayarak 0 ve 1'deki değerlerinin aynı olup olmadığını belirleyebilir.

Yukarıdaki kubitin en son değerinin $f(0) = f(1)$ durumunda hep $|0\rangle$, $f(0) \neq f(1)$ durumundaysa hep $|1\rangle$ olduğunu görmek basit bir hesapla mümkündür. Burada asıl önemli olan f – CNOT kapısının yalnız bir kez uygulanmasının, bir başka deyişle fonksiyonun yalnız bir kez hesaplanmasının yeterli olmasıdır. David Deutsch bunu paralel evrenler fikrinin doğrudan bir kanıtı olarak değerlendirmektedir. Deutsch algoritması nükleer manyetik rezonans ve iyon kapanı yöntemiyle çalışan kuantum bilgisayarlarında başarıyla uygulanmıştır.

İki işlem yerine sadece bir işlemle aynı hesabı yapabilmek çok önemli bir fark değilmiş gibi görünebilir ama kimi kuantum algoritmaları için bundan çok daha fazla hızlanma söz konusudur. Mesela kriptolojide yaygın olarak kullanılan sayıların asal çarpanlara ayrılmaları problemini, asırlardır süren çabalarla verimli bir klasik algoritma bulunamamasına rağmen, kuantum algoritmalarıyla hızlı bir şekilde çözmek mümkündür. Bir başka deyişle yeterince büyük bir kuantum bilgisayarıyla çarpanlara ayırma esasına dayalı tüm bilgi koruma engellerini aşmak mümkündür. Peter Shor'un 1994'te ortaya attığı ve daha sonra çeşitli şekillerde geliştirilen algoritma bu yüzden çok önemlidir.

İki seviyeli tüm kuantum sistemleri kubit olarak kullanılmaya adaydır. Ancak mesele sadece kubit yapmak değil çok sayıda kubiti, anlamlı işler yapabilecek bir bilgisayar için belki bin ya da daha fazlasını, bir araya getirmek, daha da önemlisi kubitleri istediğimiz hallerde hazırlayıp istediğimiz işlemleri uygulayabilmektir. İşte bunların hepsini yapabildiğimiz sistemler henüz çok sınırlıdır. Mevcut bilgisayarlarda kubit sayısı aşağı yukarı on civarındadır. Örneğin, 7 kubitli bir bilgisayarla Shor algoritmasını kullanarak 15'in 3 ve 5'in çarpımı olduğunu gösterebiliyoruz.

Kuantum bilgisayarlarının daha büyük ölçekte yapılmalarının önündeki en önemli engellerden biri bilgisayarın çevreyle etkileşim sonucu kuantum özelliklerini kaybetmesidir. Örneğin, 0 ve 1'in karışımı bir haldeki kubit, henüz hesaplamalar bitmeden indirgenir ve böylece üst üste binme özelliğini kaybederse bilgisayar istenilen işi başaramayacaktır. Bu yüzden bilgisayarların çevreden yalıtımlarına büyük özen gösterilmektedir.

Kriptoloji uygulamaları açısından önemli bir kuramsal soru, kuantum bilgisayarlarıyla bile çözülemeyen problemlerin hangileri olduğudur. Bu problemlerin saptanmasıyla kuantum algoritmalarının tehdit oluşturmadığı güvenli şifreleme yöntemleri geliştirmek mümkün olacaktır.

Yüksel Yazıcı

J.Lv.Tğm Tokat J. Blg. K.lığı
EE&Biyomedikal Y.Muh.
yuksel.yazici@boun.edu.tr

Tıbbi Uygulamalarda Uzakları Yakınlaştırmak: Teletıp

Teletıp kelime anlamıyla uzaktan-tıp ve terim anlamıyla modern haberleşme teknolojileri kullanılarak uzak mesafelere tıbbi bakım ulaştırma ve konuya bağlı sağlık bilgilerinin paylaşımı olarak tanımlanabilir. Bu tanımdan da anlaşılabileceği gibi teletıpın amacı, alanında uzman kişilerin bilgilerini, haberleşme ve bilgi teknolojileri aracılığı ile gereken yere ulaştırmak ve gerektiğinde de ileri acil kurtarma ve teşhis olanağı sağlamak. Başka bir bakış açısıyla teletıp, tanımı gereği klinik tıpta teşhis, tedavi, dokümantasyon ve akademik anlamda da araştırma, eğitim ve öğretim gibi olanaklar sağlar.



Visual Photos



cwhonors.org

Teletıp 1970'li yıllarda günümüz modern haberleşme teknolojileri öngörülerek ortaya atılmış bir kavram. Etkileşimli video görüntülü sistemler, yüksek çözünürlüklü ekranlar, yüksek hızlı bilgisayar ağları, anahtarlama sistemleri ve bunların üzerinde taşındığı fiber optik sistemler, yer-uydu sistemleri ve cep telefonu şebekeleri (GSM) gibi süper haberleşme otobanları, teletıp uygulamalarının kullanım çeşitliliğini ve etkinliğini artırmış bulunuyor.

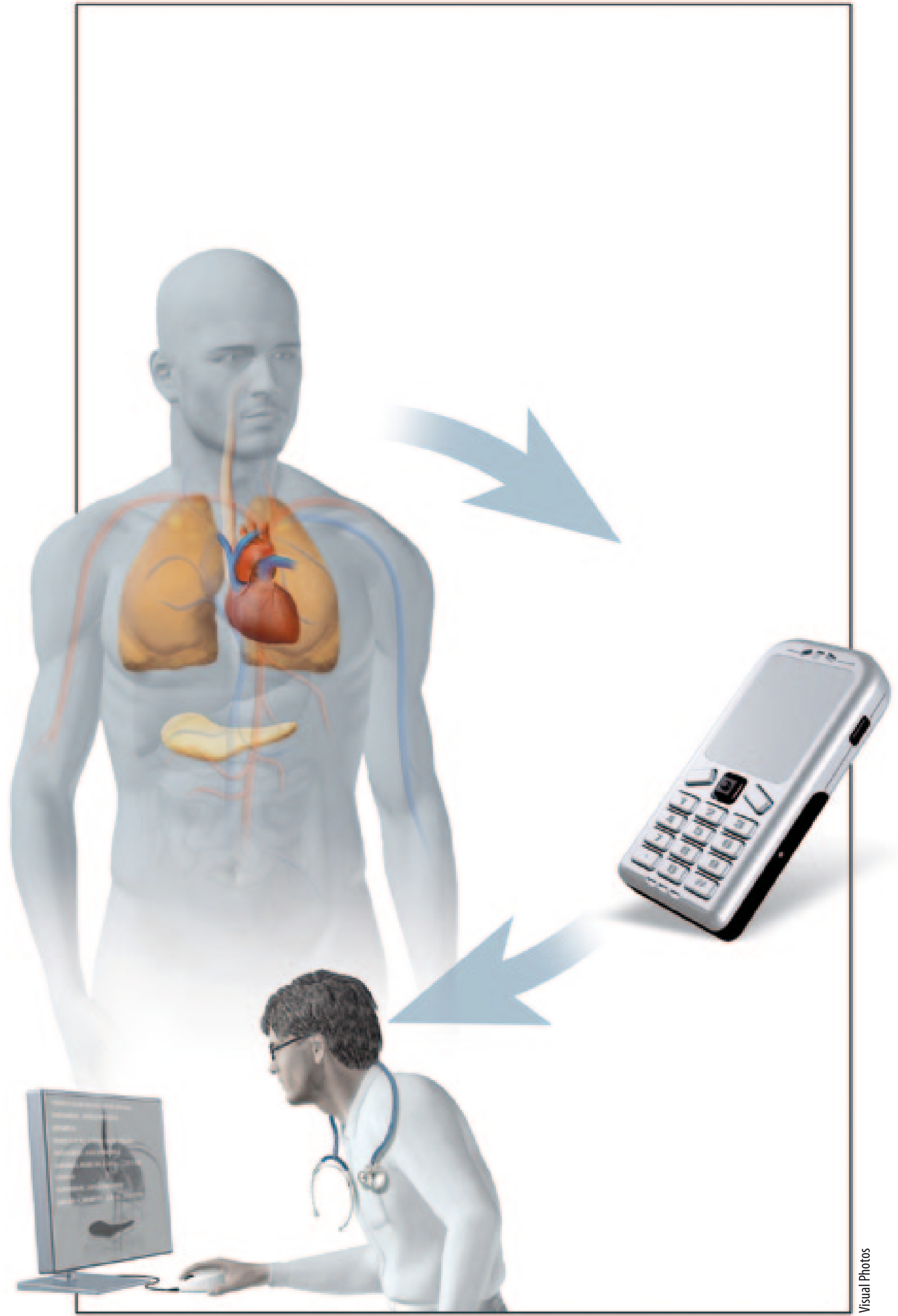
Mobil teletıp ise farklı teletıp uygulamalarının kablosuz haberleşme altyapıları ile birleştirilmesinden doğan yeni bir uygulama alanı. Bu yaklaşım bir cep telefonu üzerinden sadece sahibine

sağlanabilecek destekten veya sürekli izlenmesi gereken kronik hastaların izlenmesinden çok daha öte bir kavram: Hızla hareket eden bir cankurtaran aracındaki hastanın durumunun merkeze otomatik olarak bildirilmesi, uzmana sahip olmayan kırsal alanlara, ihtiyaç duyulan sağlık desteğinin sağlanması, doğal afet bölgelerine çok kısa sürelerde, ihtiyaç duyulan etkili ve hızlı tıbbi bilginin sağlanması, arazide dağınık halde bulunan askerlerin yaşam ve performans bilgilerini aktarabilen, sahra hastanelerine veya yaralanmalarda sıhhiye erine hastanın durum bilgisini otomatik olarak algılayarak doğru müdahale bilgisini ulaştırılmak gibi farklı kullanım alanları mevcut.

Neden Teletıp?

Bazı ciddi hastalık ve sağlık düzensizliklerinde (diyabet, kalp hastalıkları, solunum sorunları, epilepsi vb.) teşhis sonrası ölüm olasılığını azaltmak veya ileri aşamalarda daha ciddi ikincil hastalık ya da hasarlara engel olmak için sürekli ve yakın izleme gerekir. Bu hastalar, genelde hastane veya sağlık merkezlerinde barındırılarak izlenir. Fakat kalp ritmi bozukluğu ve epilepsi gibi uzun süreli izlenmesi ve kayıt tutulması gereken hastalar, sırada bekleyen diğer hastalar nedeniyle genelde erken taburcu edilir.

Hastanede uzun süren gözetim ve tedavi süreleri, neden olacağı maliyet nedeniyle hem kurum hem de hasta açısından mevcut yöntemlerin bilinen bir sorunu. Sağlık otoritelerinin çözmek zorunda oldukları en önemli sorunlardan biri de hizmet çeşitliliğini ve kalitesini artırırken maliyetleri düşük tutacak çözümler sunmak. Özellikle son 20-30 yılda hissedilmekte olan yaşlı nüfustaki artış ve bu yaşlı nüfusun beraberinde getirdiği sağlık giderlerinin bütçe üzerinde neden olduğu baskı, alternatif çözüm arayışına neden olmakta. Bu gruptaki hastaların kendi yaşam alanlarında, yaşam kalitelerine bir müdahale olmaksızın hastane olanaklarıyla gözetim altında tutulmaları ve gerektiğinde müdahalede bulunabilmesi her iki taraf için de avantajlı olur.



Visual Photos

Ameliyat öncesi ve sonrası hem hasta güvenliği hem de hastalığın seyri ile ilgili bilgi toplama olanağı sunabiliyor olması bu sistemlere olan talebi arttırmaktadır. Acil durum olarak bilinen ambulans uygulamalarında kritik müdahale sürecinde ön bilgilendirme büyük öneme sahiptir. Temel canlılık bilgilerinin servis öncesi müdahale merkezine ulaştırılması ve gerekli uzmanların ve ortamın vaktinde hazırlanmasına olacak potansiyel katkısı bu sistemleri vazgeçilmez kılar.

Teletıp geniş coğrafi alanlarda sağlık hizmetlerinin ulaştırılmasında, yönetilmesinde en etkili araçlardan biridir ve bunun en önemli nedeni modern haberleşme teknolojilerinin aktif olarak kullanılmasıdır. Sağlık altyapısı yetersiz kırsal alanlardaki kliniklerden video konferans aracılığı ile uzman sağlık merkezleri arasında kurulacak bağlantı ile teşhis ve tedavi yapılarak gereksiz hasta yolculuklarından ve maliyetlerden kaçınılabilir, vatandaş ve kurumların tedavi maliyetleri azaltılabilir.

Askeri Uygulamalar



army.mil

Askeri yaklaşımlı teletıp, 1990'ların başında NATO veya ulusal sınırlarının dışında görev yapan gelişmiş ülkelerin askeri birliklerine sağladıkları sağlık desteğini artırmak maksadıyla geliştirilmiş bir uygulamadır. Zorlayıcı arazi ve hava koşulları, düşman kuvvetleri nedeniyle belirsiz çatışma alanlarında ve hatta mayınlı arazi koşullarında bildik sıhhiye yöntemleri (ilk yardım, sedye ile taşıma vb.) ve eskort gibi tıbbi faaliyetlerde bulunmakla gereksiz risk alınır. Teletıp haberleşme mimarisi farklı bir alternatif sunar. NATO tarafından konuşlandırılmış güçler, sadece genel tıbbi desteğe sahiptir ve buralarda sıra dışı yaralanmalara, hastalılıklara ve savaş travmalarına uygun uzman kadro eksikliği yaşanmaktadır. Oysa teletıp, mantığı gereği tüm bu eksiklikleri giderebiliyor.

Halen prototip aşamasında olan bazı askeri sistemlerle komuta kademeleri üzerinden savaş alanına sağlanan sağlık bilgi akışı ile askerlerin hayatta kalma ve görevin başarı şansı artırılmaktadır. Bu sistemlerle daha önce hiç olmadığı kadar komuta kademelerinin her noktasında belli oranda personelin sağlık durumu ile ilgili önemli farkındalıklar sağlanabilmektedir. Bu süreçte en kritik aşama, askerin bireysel olarak gözlenmesi ve elde edilecek güvenilir bilginin sıhhiyeye bildirilmesidir ki bu savaş alanında tıbbi müdahalenin ilk aşamasının teşkil eder. Burada birincil hedef kitle, harekât sırasında yaşanan toplam ölümlerin %25'lik dilimini oluşturan ve yaralanmalarından sonra ilk 5 dakika ile 6 saat arasında ölen askerlerdir. Bunlar yardım ulaştırılması durumunda büyük olasılıkla hayatta kalabilecek askerlerdir ancak mevcut optimal olmayan kurtarma sistemlerinin eksiklikleri nedeniyle bu askerlerin çabucak kaybedilebildikleri görülmüştür. Araştırmalar daha etkili tıbbi bilgi akışı ile asker kaybının azaltılabileceğini gösteriyor. Diğer taraftan sıhhiyenin kurtarmaya teşebbüs ettiği vakaların %25'inin yardım ulaşana kadar zaten yaşamını yitirdiğini ve bunu yaparak sıhhiyenin kendi yaşamını da teklikeye attığı görülmüştür. Savaş alanında bazı ölümler kaçınılmazken en azından yaralanma neticesinde eksik veya geç yardım nedeniyle ölüm oranlarının düşürülmesi etkili analiz, yeterli tıbbi bilgi akışı, müdahale planlaması ve planlı kaynak (sağlık personeli ve ekipmanı) dağılımı ile mümkündür.

Savaşçıların askeri operasyonlar veya eğitimlerde fizyolojik performanslarının gözlenmesi amacıyla gerçek arazi koşulları altında kayıtları da tutulabilecek. Bu kayıtlarla, askerlerin mevcut ve çalışarak ulaşabilecekleri performanslarının belirlenmesi ve operasyon sırasında performanslarının zirvede tutulması garantisi amaçlanmakta. Gelecek nesil savaş üniformalarında savaşçının vücudu, kişiye ve göreve göre ayarlanabilen minyatür kablosuz fizyolojik algılayıcılarla donatılmış olacak. İki yönlü algılayıcı haberleşmesi ile algılayıcıların komut alışverişinde bulunabilmesi ya da duruma göre yeniden programlanması sağlanabilecek. Örneğin, mikroişlemci gömülü bir kandaki oksijen derişimi algılayıcısı ile savaş alanındaki askerin yaralanma bilgisi sıhhiye erine veya komutana otomatik olarak iletilebilecek.

Yine, vücut fonksiyonelliği için gerekli sıcaklık değerinin korunması askerin performansını devam ettirebilmesi için çok önemlidir. Bu amaçla askerin fizyolojik bilgisini vücut içine nüfuz etmeden, dışarıdan algılamaya yönelik sistemler geliştiriliyor. Özellikle hipotermiyi (düşük vücut sıcaklığını) ve maruz kalınan ısıyı belirlemeye yönelik algılayıcılar kullanılarak daha genel anlamda askerler için fizyolojik gözetleme cihazları hali hazırda üretliyor.

Kaska yerleştirilecen yüksek çözünürlüklü minyatür kameralarla teletıp haberleşme altyapısı kullanılarak araziden anlık olarak gerçek görüntü almanın karar vericiler için ne denli önemli bir avantaj olduğu açıktır. Yapılan birçok çalışma dayanıklı, güvenilir ve gerçek-zamanlı sağlık takip ve görüntüleme sistemlerinin mümkün olduğunu ve muhtemelen gelecek on yıllarda operasyonlarda kullanılmak üzere askerler için standart donanım haline geleceğini gösteriyor.

Çatışmada yaralanan veya görevi gereği sürekli taşınmak zorunda olan askeri personelin kendisine ve aile bireylerine sürekli, kaliteli ve güvenli sağlık desteği sunma ile ilgili çalışmalar dünya genelinde sürdürülüyor. Bu konu ile ilgili şimdiden bazı standartlar ve hedefler belirlenmiş bulunuyor. Elektronik Sağlık Kayıt Sistemleri, ilk müdahale ve tedavinin bütün aşamaları ile ilgili bilgilerin doktorlar ve hasta bakıcılar tarafından girilebildiği sistemlerdir. Hastanın yanından ayırmayacağı bu modüllerle veya künyelerle, hastaya şimdiye kadar uygulanan tüm tedaviler, alerji bilgileri, önceki tanılar ve yapılan testlerin sonuçları hekime sağlanabilmektedir. Hatta bu bilgilere ulaşım, sağlanacak haklarla sınırlandırılabilir.

Kablosuz videokonferans aynı zamanda, uzaktaki sağlık personelinin eğitim ve öğretimlerinin bulundukları yerden ayrılmalarına gerek kalmaksızın profesyonelce yapılabilmesine de olanak tanır. Ayrıca günümüzde yüksek hızlı haberleşme hatları üzerinden robot destekli teleoperasyonlar gerçekleştirmek artık çok daha kolay hale gelmiş durumda.

Askeri amaçlı kullanımda ülke içi ya da ülke dışı görevlerde operatif ve taktik düzeyde bireysel veya toplu teletıp hizmetlerinin sağlanabilirliği kanıtlanmıştır. Birinci ve ikinci Körfez harekâtlarında bu tür hizmetlerin cephe şartlarında verildiği ve etkinliklerinin kanıtlandığı görülmüştür.


telehealthvrc.org

Sivil Uygulamalar

Çabuk müdahale ve bir uzmanın desteği kuşkusuz sağlık hizmetlerinin etkinlik ve verimliliğini özellikle kırsal ve kolay ulaşılamayan alanlarda artırır. Acil müdahale ve evden gözetleme çözümleri, sivil kullanımda esas ilgi odağını oluşturur. Bu teknik, doğası gereği ambulanslar, kırsal alanlardaki sağlık ocakları, açık denizlerdeki gemiler vs. gibi şartları ağır ve zor her türlü ortamda kullanılabiliyor. Acil tıbbi müdahalenin gerektiği akut durumlarda hastane öncesi erken müdahale ve uzman desteğinin hastanın hayatta kalma şansını artırdığı yapılan araştırmalarla kanıtlanmıştır. Özellikle baş, omurga ya da iç organ travmaları gibi müdahale ve nakil yöntemlerinin hassas olduğu ve hastanın gelecekteki durumunu yakından ilgilendiren durumlar örnek olarak gösterilebilir.

Amerika Birleşik Devletleri'nde 1997 yılında rapor edilen 6.753.500 (nüfusa oranı %0,014) trafik kazasında 42.000 (Türkiye'de bu rakam yaklaşık 30.000 civarı ve nüfusa oranı ise %0,042'dir) insan yaşamını yitirmiş olup 2.182.660 sürücü ve 1.125.890 yolcu yaralanması olayı meydana gelmiştir. Avrupa'da ise 50.000 ölü ve yarım milyon yaralı vakası meydana gelmiştir. Bu istatistiksel bilgiler ölümlerin çoğunun yaralanmadan sonraki ilk 24 saatte, geç ve yetersiz müdahaleden kaynaklandığını ortaya koyuyor.

Kroner arter hastalıkları acil ya da evden gözetleme durumlarında sık rastlanan ve halen her üç hastadan ikisinin hastaneye ulaşamadan kaybedildiği bir diğer yüksek ölüm riskli gruptur. İngiltere'de 1998'de yapılan başka bir araştırmada ise 55 yaş üzeri kap hastalarının hastane dışında yaşadıkları kalp durmalarının %91'inin acil müdahale eksikliği nedeniyle ölümle sonuçlandığı kaydedilmiştir. Thrombolysis (pıhtılaşma veya diğer nedenlerle kalp damarının tıkanması) durumunda hayatta kalma, iğne vurulma süresine bağlıdır ki bu 60 dakikadan az bir süredir. Bu nedenle kalp krizleri ve ani kalp durmalarında acil müdahalede zaman, vakanın kurtarılması bakımından birincil faktördür. Dünya genelinde yapılan araştırmalar kanıtlamıştır ki akut kalp vakalarında hastane öncesi yapılan acil müdahalenin ölümcüllüğü azalttığı gibi tedavi süresini de azaltmaktadır. Anlaşılacağı üzere yüksek ölüm oranlarını düşürmek; yardıma ulaşma, hastane öncesi bakım ve hasta takip teknikleri ile mümkün.

Kritik bakım telemetresi başka bir acil durum takip uygulamasıdır. Buradaki yaklaşım, hastane içinde yoğun bakım ünitesindeki hastaların sürekli gözlenmesi ve aynı anda tüm telemetre bilgilerini yetkili doktora herhangi bir yerde ve herhangi bir zamanda sunmayı içerir. Yine bu yaklaşımda sorumlu doktor hastaların durumlarından 24 saat kesintisiz haberdar olabilmekte ve fiziksel olarak hastanın yanında olmasa bile hayati yönlendirmelerde bulunabilmektedir.

Teletıpta başka önemli bir uygulama alanı da evden takip veya evden gözlemedir. Hastane yerine evde sağlık servisi sağlama hem genel hasta maliyetinde düşüşü beraberinde getiriyor hem de hastanın rahatı açısından olumlu bir yerde duruyor. Normal telefon hatları üzerinden görüntü transferi yapabilen düşük ücretli televidyolar ile hastaneye gitme sıklığında belli oranda azalma sağlanıyor ve sağlık sektörü de bu hat-



ların band genişliğini ve ulaşım çeşitliliğini (GSM) artırmanın arayışı içindeler. Ayrıca farklı teşhis cihazları eklenen bu sistemlerle doktorlar hastayı görebilir ve hasta ile direkt etkileşime girebilirler. Örneğin kandaki oksijen derişimi ve respiratör (soluk, kronik broş rahatsızlığının gözlenmesinde kullanılır) akışı elektronik olarak iletilebilmektedir. Şeker hastaları kanşekeri ve insülin bilgilerini üzerlerinde taşıyacakları glukowatch (şekersaati) ile direkt olarak gönderip doktordan doğru dozaj bilgisini cevap olarak alabilmektedirler. Dahası doğum bekleyen hamile kadınlar kendilerinin bebeklerinin kalp atış bilgilerini elektronik olarak edinerek hastaheneye gönderebilir ve böylece gözetim altında kalarak gereksizce hastaneye yatırılmalarının önüne geçilmiş olur.

Küresel Teletıp Uygulamaları

Teletıp uygun durumlarda hasta tedavisine destek vermenin yanı sıra, sağlık malzemesi ihtiyaçlarının belirlenmesi ve bilgilerin hızlı bir şekilde ulusal veya uluslararası afet merkezlerine veya potansiyel bağışçı kuruluşlara (uluslararası yardım ve kurtarma çalışmalarını organize ve koordine eden yardımcı kuruluşlar) iletilmesi ve geçici yerleşim alanları için uzmanlık sağlanması, sıhhi mühendislik, su kaynağı, afet nezareti-kontrolü gibi halk sağlığını ilgilendiren konularda da destek verir.

Son zamanlarda biyolojik kitle imha silahlarının kullanılabilme olasılığındaki artış, mevcut afet gözetleme sistemlerinin acilen gözden geçirilmesine neden olmuştur.

Aslında kırsal alanlarda karşılaşılabilecek, doğal yolarla oluşan sayısız biyo-tehdit vardır. Buna karşılık zararlı materyallere karşı gerekli eğitimi almış çok az sayıda uzman ekip mevcuttur ve çoğu da nufus yoğunluğunun ve tehdit olasılığının daha fazla olması nedeniyle şehirlerde konuşlandırılmışlardır. Afet yönetimi ile ilgili geliştirilen sistemler kurban arama, kimlik tespiti ve tahliye edilecek bölgelerin tahliye seviyesinin tespiti ile sorumludurlar. Bu ekipler yerel olarak kaydettikleri bilgileri geçici veya gezgin arazi hastanelerindeki operatörlere iletmek üzere genelde mobil telefonlar veya cep bilgisayarlarıyla ile donatılmışlardır. İlk tıbbi yardımı yapacak ekiplerse hedef sağlık bilgilerini merkeze veya mobil arazi hastanesine ulaştırmak için kayıt ve iletim amaçlı mobil teletıp çalışma istayonlarıyla donatılmışlardır. Afet bölgesi yakınlarına konuşlandırılmış böyle bir hastane ile mobil ekiplerle koordineli bir şekilde tıbbi duruma bağlı olarak kurbanların kurtarılma önceliğinin belirlenmesi, ilk yardımda bulunma ve daha ileri uzman görüşüne ihtiyaç duyulduğunda video konferans bağlantı ile merkezi hastaneden destek alma faaliyetleri yürütülür.

Bilgi teknolojilerinin sağlık sektöründe kullanılması çok fazla sayısal bilgi birikmesine neden olacaktır. Potansiyel olarak dünya genelindeki tüm hastaların bilgilerini içerecek böyle bir depolamaysa çok daha büyük boyutlarda olacaktır. Diğer taraftan bu bilgi zenginliği, profesyonellerine çok değerli fırsatlar da sunacaktır. Yakın gelecekte akıllı giysiler ve konu edilen sağlık desteği ile ilgili yeni iş alanlarının doğacağını tahmin etmek zor değildir. Bireysel veya organizasyonel anlamda yeni haberleşme ve iletişim teknolojilerinin sağlayacağı olanaklar açık. Sayısal ses, görüntü ve resim iletimi, kırsal ve alt yapı eksikliği yaşanan yerlerde kaliteli sağlık desteği, izole bölgelerdeki pratisyenlere merkezi hastanelerle bağlantı olanağı, evlere sağlık bilgisi ve desteği ulaştırma, hastaları evlerinden izleme, hastayı toplum içinde tutarak bakım sürekliliği sağlama, sağlık personelinin ve hastaların ulaşım ve harcamalarında azalma, yeni iş alanı fırsatları gibi sivil ve askeri kullanım potansiyeli bulunmaktadır.


ESA

Sağlık sektöründe payını hızla artırmakta olan bir diğer konu yaşlıların evden bakımıdır. Sağlık ve özellikle de "evde sağlık" sektörü, verimliliğini artırmak için rutin hemşire ziyaretleri yerine bazı hayati sinyalleri uzaktan elde etme yoluna gidiyor. Aile hekimleri, hasta evinin değişik noktalarına (akıllı yatak, akıllı tuvalet, akıllı klima ve akıllı tartı) yerleştirilmiş elektronik algılayıcıların sağlayacağı değerli bilgilerle sürekli hastasını izleyebilir. Hastaya temas etmeyen bu mikro algılayıcılarla toplanan yaşamsal bilgiler bir merkeze toplanır. Böylece aboneden (hastadan) kilometrelerce uzakta olabilecek sağlık hizmeti sunucuları hastanın nabız, kan oksijenlenmesi, vucut sıcaklığı, soluk alıp-verme ve idrar tahlili gibi bazı temel yaşamsal işaretlere bakarak sürekli bir genel sağlık kontrolü gerçekleştirmiş olur.

Doğru tedavinin seçilebilmesi için normal bir gün içerisinde hareketlerinin uzun sürelerle gözlenmesi gereken epilepsi, parkinson vb. hastalarını GSM tabanlı cep telefonlarına eklenecek veri kartı ile takip etmek mümkün. Bilindiği gibi evde yatan hastalara acil durumlarda ilk müdahaleyi yapacak olan personel hasta bakıcılar veya hemşirelerdir ve bu kişilerin olası her durum için gerekli müdahalenin teorik arka planını bilmeleri veya yeterli tecrübeye sahip olmaları beklenemez. Fakat acil teletıp ve evde izleme sistemleri, kardiyolog, beyin cerrahı, ortopedi uzmanı gibi uzman kişileri bünyesinde barındıracağı için olası acil durumlar kotarılabilecektir. Halen kullanılmakta olan bu tip telsiz sistemlerle hastanın hayati bilgilerini ve anlık panoramik görüntülerini uzman doktorlara ulaştırılabilmek ve gerektiğinde hastaya verilecek ilaçların dozlarını da uzaktan değiştirebilmek mümkün.

Akıllı elbiseler sivil ve askeri bir çok sağlık takibi uygulamasında kulanım potansiyeline sahip. Sağlık takibinde akıllı elbiselerin kişiye özel belli sağlık bilgilerinin ve yaşamsal bazı temel sinyallerin gözlenmesi için programlanabilir özellikte olacakları düşünülüyor. İzlenen bilgiler yine elbise içinde işlenebilir ve gerektiğinde müdahale edilebilir. Bu elbiselerin ağrı ya da sancının kaynağını tam olarak belirleyebilecek özellikte olacağı öngörülüyor. Bu yelekler, durumun ciddiyetine bağlı olarak sağlık desteği alınan baz istasyona otomatik çağrı yaparak bilgi verebilecek. Bu akıllı elbiseler özellikle yaşlı kişiler için çok faydalı olacak. Ancak birçok girişimci şimdiden modaya ve ergonomiye uygun tasarımlar ve ihtiyacı karşılayacak teknolojik kabiliyetleri belirleme ve uygun pazar arayışlarına girmiş bulunuyor.



esri.com

Afet Uygulamaları ve Diğer Uygulamalar

Teletıp'ın farklı kullanım alanlarından biri de afet-doğal afet türü (deprem, sel, yangın, tren veya otomobil kazaları; virüs, kimyasal veya biyolojik saldırılar vb.) olayların yaşandığı durumlardır. Afete ilk reaksiyon göstererek bölgeye intikal edecek bu ekipler de muhtemelen çevre şartlarından olumsuz etkilenir, çünkü afetin boyutlarına bağlı olarak haberleşme sistemlerinin (PSTN, kablolu hatlar veya GSM) de çöktüğü durumlar yaşanır. Bu durumda sağlık desteği için gerekli bağlantı uydu üzerinden yapılır. Afet durumlarına ilk müdahale edecek ekiplerin durumu ile ilgili farklı görüşler de mevcut. Örneğin kimine göre afet bölgesine gidecek olan ekibin dışarıdan desteğe ihtiyacı olamaması gereken uzmanlardan oluşması gerekir. Ancak bunun gerçekte her zaman mümkün olamayacağı da kesin. Afet alanlarında yapılacak ilk şey, işi seçmektir çünkü karşılaşılacak karmaşık bir durumda yardım etme içdügüsü ile kaybedilecek zaman zarfında başka bir yerde yaşamlar kurtarılabilir.

Dünya Acil Haberleşme Çalışma Grubu'nun (WGET) uzmanlarına göre teletıp, "en akut zamanlarda veya sorunu çözmek için daha fazla zaman olduğu durumlarda teşhis gibi problemlerin çözülmesinde uzmanlardan danışmanlık almaktır" şeklinde tanımlanıyor. Ne var ki, ihtiyaç duyulan danışmanlık alındıktan sonra bile, çoğu kez alınan bu teknik desteğin uygulanması aşamasında yerel sağlık görevlilerinin (ilk sağlık müdalesini yapacak personel) kapasitelerinin yetersiz kaldığı görülüyor.

Kaynaklar

http://www.bme.boun.edu.tr/biyomut/Biyomut_Sunumlar/biyomut%202005/sunumlar/53.%20MOB%C4%B0L%20TELEFON%20KULLANARAK%20TRANSTELEFON%C4%B0K%20EKG%20VE%20SICAKLIK%20%C3%96L%C3%87%C3%9CM%C3%9C%20YAPAB%C4%B0LEN%20B%C4%B0R%20C%C4%B0HAZ%20TASARIMI.pdf

http://www.openecg.net/WS2_proceedings/Session07/S7.1_PA.pdf

http://www.ece.uah.edu/~jovanov/papers/rmbs01_wireless.pdf

http://www.biomedical-engineering-online.com/content/2/1/7

http://www.onk.ns.ac.yu/Archive/Vol9/PDFVol9/V9n2p111.pdf

*Nursel Aşan**

*Damla Ateş***

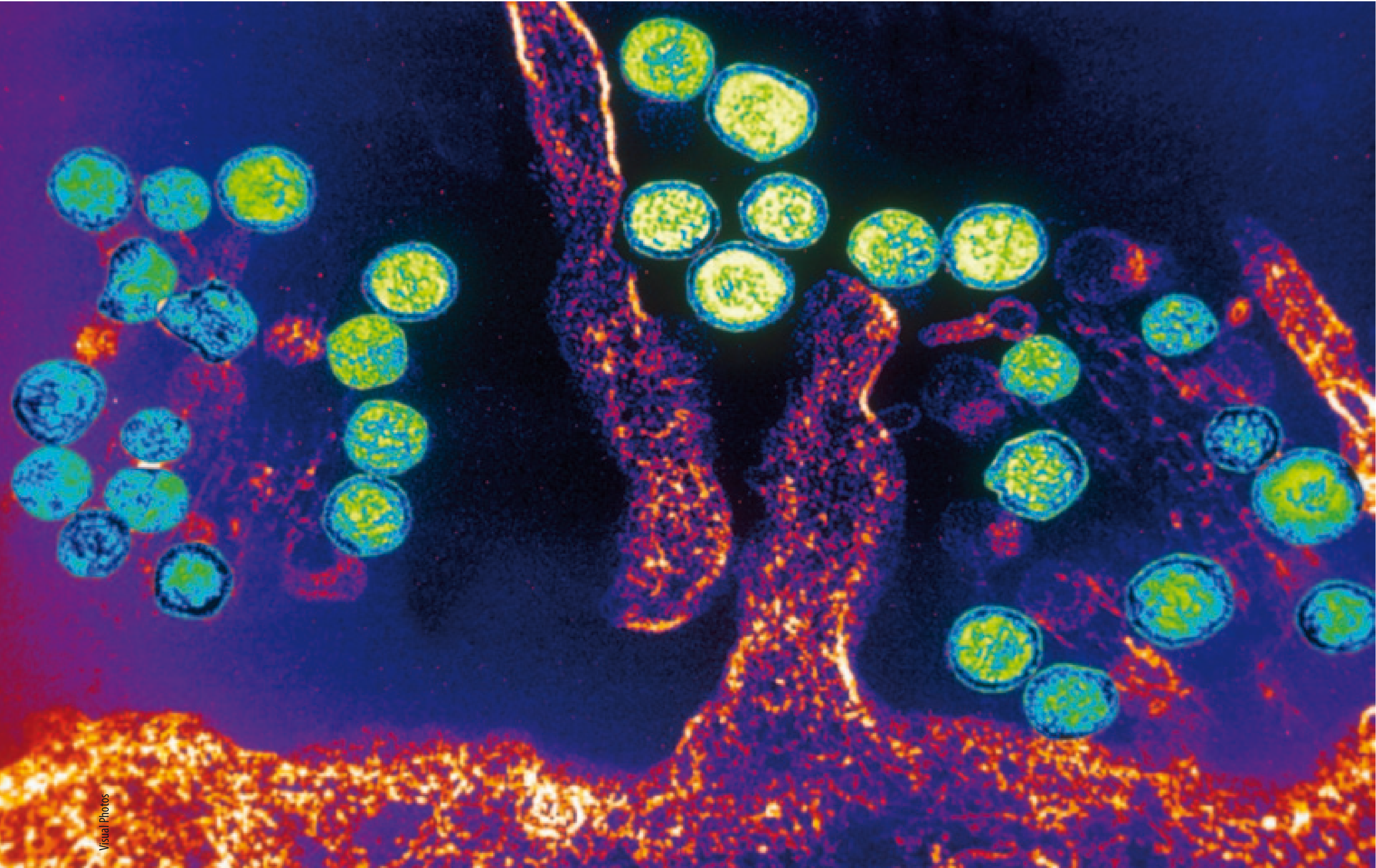
**Yrd. Doç. Dr.,*
***Yüksek Lisans Öğrencisi,*
Kırıkkale Üniversitesi,
Fen-Edebiyat Fakültesi
Biyoloji Bölümü

Hanta Virüsü

Son birkaç aydır medyada Hanta virüsünden kaynaklandığı düşünülen ölüm vakalarıyla ilgili haberlere rastlıyoruz. Ülkemizde yeni duyulmasına karşın, bu virüs türünün Asya ve Amerika'da insanlarda neden olduğu hastalıklar yıllardır biliniyor.

Hanta virüsü, Bunyaviridae familyasına ait bir RNA virüsüdür. Bu familyadaki Bunyavirüs, Phlebovirüs, Nairovirüs ve Tospovirüs eklembacaklılar tarafından taşınırken, Hanta virüsü kemirici türlerle taşınıyor. Sivrisinekler tarafından taşınan Bunyavirüs özellikle çocuklarda merkezi sinir sistemini etkileyen "La Crosse Encephalitis" (beyindeki akut iltihap) hastalığına yol açıyor. Yine sivrisineklerce taşınan Phlebovirüs sığır, bufalo, koyun, keçi ve deve gibi toynaklı memeliler ile insanlarda, ateşli bir hastalık olan "Rift vadisi humması"na neden oluyor. Nairovirüs kenelerle taşınıyor ve artık hepimizin bildiği "Kırım Kongo Kanamalı Ateşi" hastalığını tetikliyor. İnsanlarda herhangi bir hastalığa neden olmayan Tospovirüs ise etkisini bitkilerde gösteriyor.

Çapı 80-120 nanometre olan Hanta virüsü elektron mikroskobunda küresel veya oval olarak görünüyor. Birçok hayvan virüsünde olduğu gibi hanta virüsü de genetik materyali çevreleyen proteinden oluşmuş bir nükleokapsit ve bu kapsitin etrafında viral bir zarfa sahip.



Visual Photos

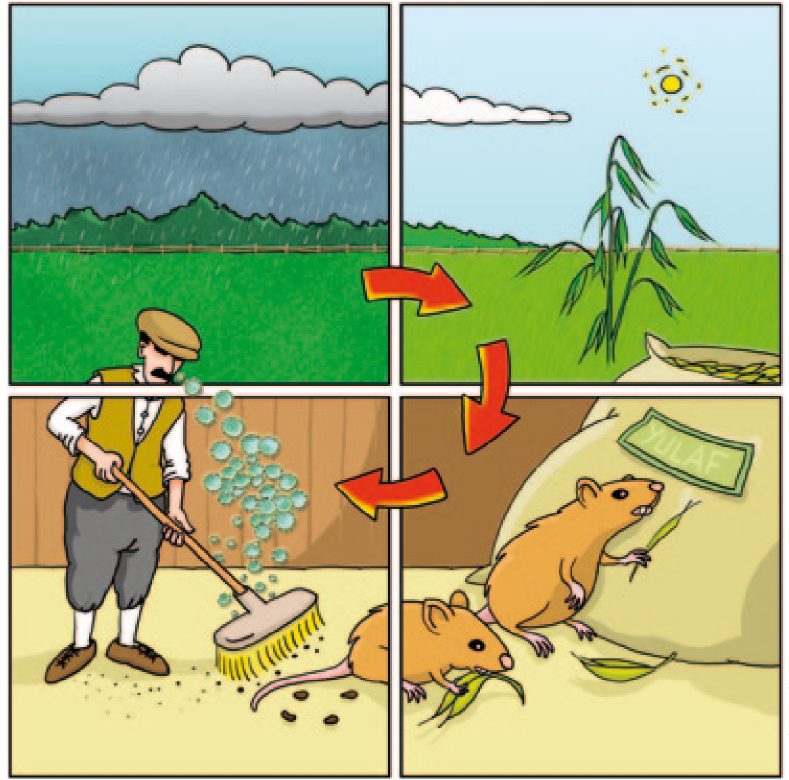
Hanta virüsüyle enfekte olmuş kemiriciler bu virüsü akut veya kronik belirtiler göstermeden, haftalar, aylar, yıllar ve hatta tüm ömürleri boyunca taşıyabiliyorlar. Popülasyonda bir bireyden diğerine geçiş hayvanların birbirlerini ısırmasıyla gerçekleşiyor. Hastalıklı hayvanın tükürüğünde, idrarında ve dışkısında bulunan virüs insanda iki tip hastalığa neden oluyor:

- Böbrek Yetmezliğiyle Seyreden Kanamalı Ateş (HFRS)
- Hanta Virüsü Kalp-Akciğer Sendromu (HPS)

Tarihçe

MÖ 960'ta Çin'de, ortaçağda İngiltere'de Hanta virüsünün neden olmuş olabileceği hastalıklarla ilgili kayıtlar bulunuyor. Buna karşın Hanta virüsü hastalıklarının ilk klinik kayıtları 1913'te alınıyor. Virüsün neden olduğu hastalıklar ilk kez 1913 ve 1932 yılları arasında Rusya'da "*Böbrek Yetmezliğiyle Seyreden Kanamalı Ateş*", 1934'te İsveç, Norveç ve Finlandiya'da "*Nephropathia epidemica*" ve 1950'li yıllarda Kore Savaşı sırasında "*Kore Kanamalı Ateşi*" (bu isim artık kullanılmıyor) olarak kaydedildi. Virüs kemiricilere temas eden asker, çiftçi gibi daha çok erkek bireylerde hastalık etkeni olmuştur. 1976 ve 1978 yılları arasında Dr. Lee Ho-Wang ve çalışma arkadaşları Çizgili orman faresinin (*Apodemus agrarius corea*) akciğer ve böbreklerinde bir virüs izole ettiler (ayırdılar) ve buna "Hantaan" adını verdiler. Sonraki yıllarda kemiricilerin yanı sıra böcekçillerden de yeni virüs tipleri izole edildi ve bulundukları bölgeye göre adlandırıldılar. Ortadoğu'da kaydedilen herhangi bir klinik vaka bulunmuyor. Yakın bir zamanda Afrika tahta faresi'nden (*Hylomyscus simus*) bir virüs izole edildi. Avustralya kıtasında da Hanta virüsü kaynaklı bir hastalık kaydedilmiş değil, fakat araştırıcılar burada yayılış gösteren kemirici türlerinde virüsün bulunabileceğini düşünüyor.

Hanta Virüsü Kalp-Akciğer Sendromu (HPS) ilk kez 1993'te ABD'nin Kolorado, Utah, Arizona ve New Mexico eyaletlerinin birleştiği Four Corners bölgesinde görüldü. Araştırıcılara göre HPS salgını Four Corners'da meydana gelen iklim değişimlerine dayanıyor. 1993'ten önce bu bölgede birkaç yıl süren kurak bir dönem yaşandı. 1993 ilkbaharında başlayan yoğun yağmur ve kar yağışları o yıl bitki ve hayvan popülasyonlarında artışa neden oldu. Mayıs ayında kemirici sayısı bir önceki yıla göre on kat artmış bulunuyordu. New Mexico Eyaleti'nde kemiricileri kutsal sayan Navaho yerli halkı ani ateş, kramp, baş ağrısı, öksürük ve bunları izleyen akciğer ödemi, solunum yetmezliği, düşük tansiyon belirtileriyle hastanelere başvurdu. Haziran ayına gelindiğinde 12 kişi hayatını kaybetmiş bulunuyordu. Yetişkinlerde görülen bu hastalığı araştırıcılar Akut Solunum Sıkıntısı Sendromu (ARDS) olarak adlandırdılar.



Çizim: Bilgin Ersözlü

Yağışın bol olduğu yerlerde besin kaynaklarında artış gerçekleşir. Artan besin, kemirici popülasyonlarındaki birey sayısında da artışa neden olur. Virüsle enfekte olan kemiricilerin beslendikleri yerlerde bıraktıkları dışkı, tükürük ve idrar Hanta virüsünün yayılışını kolaylaştırır ve virüs içeren tozları süpüren bir kişinin vücuduna solunum yoluyla girer. Ayrıca kemirici türleri üzerinde çalışan araştırıcılar, hastalıklı deneklerin ısırığına maruz kaldıklarında Hanta virüsü kapabilirler.

Hanta Virüsü İnsanlara Nasıl Bulaşır?

Hanta virüsleri canlı bir birey ya da organik bir materyal içinde uzun süre yaşarlar. Puumala ve Tula virüsleri oda sıcaklığında (23°C) 24 saat içinde yok olur. Ancak bulundukları ortam sürekli nemli kalırsa yaklaşık beş gün etkinlik gösterebilirler. Virüsler çatlak deriden, gözden, ağız, burnun içi, mide, barsak, akciğerler gibi alanları döşeyen membrandan ve kemirici ısırığı ile yenen besinler yoluyla insana geçer. İnsandan insana geçtiğine dair kayıtlar yalnızca Arjantin'de Andes virüsünün bulaştığı bireyleri kapsamaktadır ve bu kayıtlarda anne sütünden bebeğe geçebildiği de belirtilmiştir. Kemirici ve böcekçiller dışında yarasa ve domuz gibi bazı memeliler de Hanta virüsüyle enfekte olabilmektedirler, fakat bu hayvanların hastalandıklarına dair henüz yeterli kayıt bulunmuyor. Kedi, köpek, domuz, at, sığır, geyik, tavşan ve çakal, bazı Hanta virüsü tiplerine karşı antikor taşıdığı tespit edilen memelilerdir. Rusya'da yapılan bir çalışmadaysa çeşitli kuş türlerinin ciğerlerinde Hanta virüsü antijenine rastlanmıştır.

Kimler Risk Altındadır?

- Kemirici yuvalarına yakın ev veya işyerlerinde bulunan kişiler
- Hastalık taşıyan kemiricilere eldivensiz dokunan kişiler
- Hastalık taşıyan kemiricilerin dışkı-idrar-tükürük bıraktıkları alanlarda gezen ya da kamp kuran kişiler
- Gemilerde ve limanlarda çalışan işçiler
- Temizlik işçileri
- Toprak üstünde uyuyan ya da toprağa çıplak elle bitki diken kişiler
- Kemiriciler üzerinde çalışan bilim insanları

Sarı boyunlu orman faresi
(*Apodemus flavicollis*)



Visual Photos

İnsanda Böbrek Yetmezliğiyle Seyreden Kanamalı Ateş'in Belirtileri

Böbrek Yetmezliğiyle Seyreden Kanamalı Ateş (HFRS) hastalığına yakalanan kişilerde virüs kanda veya idrarda görülmektedir. Virüsün kuluçka süresi 1-6 haftadır. Puumala ve Dobrava virüslerinden meydana gelen HFRS'nin klinik ve laboratuar belirtileri birbirinden farklılık gösterir. Hastalığın ilk belirtileri yorgunluk, şiddetli sırt, kas ve karın ağrısı, bulantı, kusma ve yüksek ateştir. Sonra görülen belirtilerse gözlerde kanama, ağrılı şişlik veya kızarıklık ile kronik böbrek yetmezliği ve düşük tansiyondur. Hastalığın şiddeti hastalığa neden olan virüse bağlı olarak değişir. Seoul ve Puumala türlerinden kaynaklanan enfeksiyonlar genellikle orta şiddette seyrederken, Hantaan ve Dobrava türlerinden kaynaklanan enfeksiyonlar daha şiddetli belirtilere yol açmakta ve iyileşme süreci aylarca sürebilmektedir. Bu hastalıktan ölüm oranı % 6-15 arasındadır.

İnsanda Hanta Virüsü Kalp-Akciğer Sendromu'nun Belirtileri

Hanta Virüsü Kalp-Akciğer Sendromu (HPS) ateşli bir hastalıktır. Virüsün kuluçka süresi türüne göre 7-39 ya da 9-33 gün olabilmektedir. Hedef organ akciğerdir. Virüsü kapan kişideki ilk belirtiler soğuk algınlığı belirtilerine benzer şekilde yorgunluk, yüksek ateş (38°C ve yukarısı), kas, karın ve baş ağrısıdır. Bu belirtileri izleyen 4-5 gün içinde damar içi geçirgenliğin artması nedeniyle iki yönlü akciğer ödemi, tansiyon düşüklüğü, nefes darlığı ve öksürük baş göstermektedir. Hastalık hızlı bir şekilde ilerlediği için hastaya 24 saat içerisinde müdahale edilmesi gerekir. Aksi takdirde 48 saat içerisinde ölüm gerçekleşmektedir. HFRS'den daha ender görülmekle birlikte ölüm oranı % 50'dir.

Hanta Virüsü Kalp-Akciğer Sendromu görülen hastalara oksijen tedavisi yapılır. Böbrek Yetmezliğiyle Seyreden Kanamalı Ateş görülen hastalarsa diyalize sokulur. Her iki durumda da hastaya antiviral bir ilaç olan Ribavirin verilir.

Hanta virüsü enfeksiyonu teşhisinde;

- Serum ya da plazma örneklerinde Enzim İlintili İmmün Test (ELİSA)
- İndirekt İmmunfloresan Antikor Testi (IFAT)
- Enzim İmmuno Assay (EIA)
- İmmunoblot
- İmmünohistokimyasal
- Kinetik Revers Transkriptaz Polimeraz Zincir

<<<

Reaksiyonu (RT-PCR) (nükleik asit dizi analizi) yöntemleri kullanılır.

Bazı kaynaklara göre Hanta virüsüne karşı aşı yoktur diğer kaynaklara göreyse aşı geliştirilmiş ama satışa sunulmamıştır. Böbrek Yetmezliğiyle Seyreden Kanamalı Ateş (HFRS) için Kore'de bir aşı kullanılmakla birlikte bu aşının ne derece koruyucu olduğu halen tartışma konusudur.

Ülkemiz Hanta virüsü ile ilk kez 1997'de, bazı diyaliz hastalarında virüse ait antikorların saptanmasıyla tanıştı. 2004-2005 yılları arasında yapılan serolojik (serum bilimiyle ilgili) başka bir çalışmadaysa Trabzon, Rize ve İzmir illerinde yakalanan kemirici örneklerinden, 65 tarla faresinin sadece 4'ünde Puumala virüsü antikoru tespit edildi. Bu yılın Şubat ve Nisan aylarında Zonguldak ve Bartın illerinde Hanta virüsü şüphesiyle hastanede tedavi gören 18 kişiden ikisi Böbrek Yetmezliğiyle Seyreden Kanamalı Ateş bulgularıyla hayatını kaybetti. Bu kişilerden birinin Refik Saydam Hıfzıssıhha Enstitüsü ve Dokuz Eylül Üniversitesi Tıp Fakültesi'nde incelenen ön testlerinde virüs çıkmamıştır. Bu hastanın Hanta virüsü kaynaklı bir hastalıktan ölüp ölmediği halen tartışma konusudur. Ülkemizde Hanta virüsüyle ilgili araştırmalar Refik Saydam Hıfzıssıhha Enstitüsü, Dokuz Eylül Üniversitesi Tıp Fakültesi, Zonguldak Karaelmas Üniversitesi Tıp Fakültesi, Sağlık Bakanlığı, Hacettepe Üniversitesi Tıp Fakültesi, Zonguldak İl Sağlık Müdürlüğü ve Bartın İl Sağlık Müdürlüğü'nde yapılmaktadır.

Türkiye'de *Sorex araneus* (Orman sivri faresi), *Microtus arvalis* (Orman faresi), *Clethrionomys glareolus* (Kısa kuyruklu kızıl orman faresi), *Apodemus flavicollis* (Sarı boyunlu orman faresi), *Apodemus agrarius* (Çizgili orman faresi), *Rattus norvegicus* (Norveç sıçanı veya göçmen sıçan) ve *Rattus rattus* (Ev sıçanı) türleri yayılış göstermektedir. Doğada kemirici türleriyle beslenen yılan gibi sürüngenler, baykuş ve diğer yırtıcı kuşlar ile etçil memeliler kemirici popülasyonunu dengede tutar. Avcı sayısı azaldığında hızla artış gösteren kemiriciler yaşadıkları ormanlık ve ekili alanlardan, daha kolay besin bulabilecekleri insanlara ait yaşam alanlarına yayılmaya başlar. Bu nedenle sadece ülkemizde değil tüm dünyada doğal dengenin korunmasında kemiricilerle beslenen hayvanlar çok önemlidir.

Ülkemizde Hanta virüsünün yayılmasını engellemek için gerekli diğer bir önlem de bu virüsün neden olduğu hastalıkların daha sık görüldüğü Uzakdoğu ülkelerinden ticari amaçla gelen tır ve gemilerin sıkı bir şekilde kontrol edilmesidir.

Hangi Önlemler Alınmalıdır?

Kemirici popülasyonunun kontrolü, Hanta virüsü kaynaklı hastalıkları engellemek için ilk stratejidir.
Diğer önlemler ise şöyledir:

- Kemiriciler mümkün olduğunca evlerden uzak tutulmalı,
- Kemiricilerin bulunduğu yerlere dokunulduğunda eller sabunla yıkanmalı,
- Üzerine fare idrarı ya da dışkısı bulaşan giyecekler deterjanlı sıcak suda yıkanmalı,
- Evlerde bulunan ölü kemiriciler çıplak elle tutulmadan, derin bir çukur kazılarak toprağa gömülmeli ve bulunduğu yer seyreltilmiş çamaşır suyuyla silinmelidir.

Ayrıca,

- Yiyecek ve içecekleri kapalı bir şekilde, kemiricilere dayanıklı saklama kaplarında saklamak,
- Evcil hayvanlara yeteri kadar yiyecek vermek ve kalan yiyeceği bekletmeden atmak,
- Evcil hayvanlara geceleri fazla miktarda yiyecek ve içecek bırakmamak,
- Çöp kutularının içini ve dışını sık sık sabunlu suyla yıkamak,
- Yemek tabaklarını bekletmeden yıkamak,
- Kemiricilerin yuva yapmasını kolaylaştıran pamuk, gazete vb. şeyleri ortada bırakmamak,
- Hasarlı boruları tamir etmek,
- Dış kapı ve pencereleri kapalı tutmak,
- Kemiricilerin eve girebileceği yerlere tuzaklar yerleştirmek,
- Odun yığını, ağaç yığını, tuğla, taş veya diğer malzemeleri evin uzağında tutmak,
- Çöpleri kemiricilere dayanıklı çöp kutularında saklamak,
- Çimleri kısa biçmek ve biriken çim yığınlarını bekletmeden atmak gerekmektedir.

Bunlara ek olarak,

- Temizlik yaparken lastik, lateks, vinil veya nitril eldivenler giyilmeli,
- Yerdeki tozlar etrafa yayılmadan ıslatılarak süpürülmeli,
- Kemiricilerin bulunduğu alanlar dezenfektanlar veya % 10 seyreltilmiş çamaşır suyuyla temizlenmelidir.



Kaynaklar

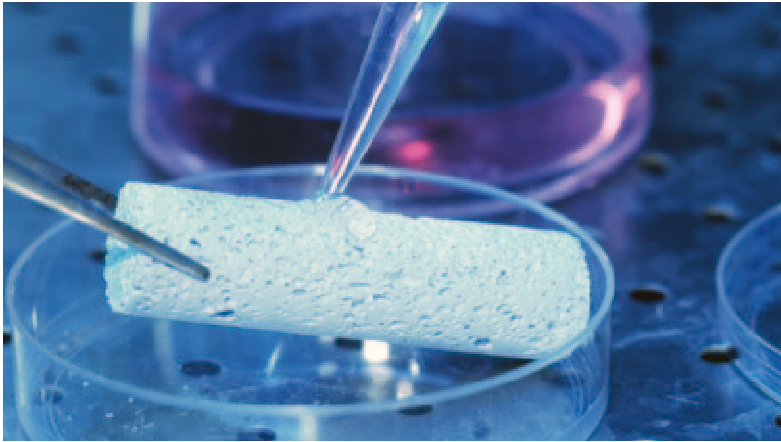
http://www.cdc.gov/ncidod/diseases/hanta/hps/noframes/outbreak.htm
http://www.cdc.gov/mmwr/PDF/rr/rr5109.pdf
http://www.cdc.gov/ncidod/dvrd/spb/mnpages/HPS_Brochure.pdf
http://www.cdc.gov/ncidod/diseases/hanta/hanta94.htm
http://www.cdc.gov/ncidod/diseases/hanta/hps/noframes/generalinfoindex.htm
http://www.nsf.gov/news/special_reports/ecoinf/images/Hantavirus2.jpg
http://www.cdc.gov/ncidod/diseases/hanta/hps/noframes/generalinfoindex.htm
http://www.cdc.gov/ncidod/diseases/hanta/hps/noframes/outbreak.htm
http://images.search.yahoo.com
http://www.cfsph.iastate.edu/Factsheets/pdfs/hantavirus.pdf
http://www.iha.com.tr/haber/Saglik
http://www.ncbi.nlm.nih.gov
http://www.rshm.gov.tr
http://www.haberinyeri.net/Saglik/Hanta-virusune-dikkat_56797.html
Anonim, "Hantavirus disease," *Ann. Soc. Belge. Med. Trop.*, Sayı 67: 89-92, 1987.
Yates, T.L. ve diğerleri, "The Ecology and Evolutionary History of an Emergent Disease: Hantavirus Pulmonary Syndrome," *BioScience*, Sayı 52 : 990-998, 2002.
Delfraro, A. ve diğerleri, "Yellow Pygmy Rice Rat (Oligoryzomys flavescens) and Hantavirus Pulmonary Syndrome in Uruguay," *Emerging Infectious Diseases*, Sayı 9: 846-852, 2003.
Campell, N.A. ve Reece, J.B., *Biyoloji*, Palme Yayıncılık, 2006.

Mustafa Özgür Güler

Yrd. Doç. Dr., UNAM-Malzeme Bilimi ve Nanoteknoloji Enstitüsü Bilkent Üniversitesi

Doku Mühendisliği ile Yedek Organlara Doğru

Dünyada ve ülkemizde, organ yetmezliğinden dolayı hastanelerde tedavi gören ve organ bağışıiçin sıra bekleyen pek çok hasta bulunmaktadır. Organ naklinin yapılabilmesi için uygun bağışçıların bulunabilmesi çok uzun ve acılı bir süreçtir. Operasyon sonrasında da nakledilen organı vücuda kabul ettirebilmek için yan etkileri kaçınılmaz olan, bağışıklık sistemini zayıflatıcı ilaçlar kullanılır. Son yıllarda yapılan, doku mühendisliği alanındaki bazı çalışmalar organ naklindeki zorlukların aşılması için ümit veriyor. Bu çalışmalar neticesinde, yakın zamanda doku mühendisliği çalışmaları ile yapay organlar üretilmesi mümkün olabilir. Doku mühendisliği alanında çok hayati önemi olan sağlık ürünlerinin üretilmesi için, doktorlar, kimyagerler, biyologlar ve malzeme mühendisleri ortak çalışmalara imza atıyorlar.



Doku mühendisliğinin yaklaşımı, hastaya göre tedavi odaklı olduğu için yan etkilerin mümkün olan en az seviyede olması beklenir. Doktorlar hastalardaki rahatsızlıkları tespit ettikten sonra biyologlara bu sorunun temelinde yatan biyolojik bilgi için danışırlar. Buradan elde edilen bulgularla sorunun ne olduğu ve tedavi için gerekli olan yöntemle ilgili ihtiyaçlar belirlenir. Daha sonra kimyagerler ve malzeme mühendisleri gerekli olan araçları ve ilaçları üretmek için çalışmalar gerçekleştirirler. Geliştirilen araçlar doktorlara iletilir ve hastalıklara çareler bulunmaya çalışılır. Doku mühendisliği, mümkün olan en iyi çareyi bulmak için biyolojik mekanizmanın nasıl çalıştığına, biyolojik etkileşimlere müdahale etmek için nasıl davranmak gerektiğine uzmanlık seviyesinde hakim olmalıdır. Hassas etkileşimlerin en küçük ayrıntılarına kadar öğrenilmesi ve dikkat edilmesi başarıya ulaşmada büyük önem taşımaktadır.

Doku mühendisliğinde tedavi için ilk baş vurulan yöntemlerden birisi vücuttaki hasta bölgeye büyüme faktörleri gibi bazı biyo-aktif moleküllerin doğrudan enjekte edilmesidir. Büyüme faktörleri hücre gelişimi ve çeşitlenmesi mekanizmalarında görev yapan doğal proteinlerdir. Büyüme faktörlerinin doku oluşumunda önemli rolü olduğu bilinmektedir. Vücudun farklı bölgelerinde hasarları tamir etmekte farklı büyüme faktörleri görev almaktadır. Örneğin, kemiklerde oluşan kırık ve çatlakların tedavi edilmesinde, kemik hücrelerinin gelişimini sağlamak için kemik morfojenez proteinleri gerekmektedir. Kemikte oluşan hasarın giderilmesinin mümkün olmadığı ya da iyileşmenin çok yavaş olduğu durumlarda, kemik büyüme faktörleri doğrudan hasarlı bölgeye uygulanarak kemik hücrelerinin hasarı tamir etmesi sağlanır.

Bazı ciddi rahatsızlıklarda, tedavi için sadece biyo-aktif moleküllerin doğrudan enjeksiyonu yeterli olmayabilir. Bu durumlarda daha etkin bir tedavi için hastadan alınan sağlıklı hücrelerin çoğaltıl-

ması yöntemiyle yeni doku oluşumu sağlanır. Hücreler sağlıklı yaşayabilmek için doğal ortamlarına benzeyen yapay bir matris içinde bulunma ihtiyacı hissederler. Bu matris hücrelerin yaşaması için gerekli olan besin, oksijen ve mekanik desteği sağlamalıdır. Bir başka deyişle hücreler ile aynı dili konuşabilecek bir malzeme oluşturulması gerekir. Bu malzemenin tasarımı için en önemli model, doğal hücreler arası ortamdır. Yapay matrisler, hücrelerin yaşamsal faaliyetlerinin devamını sağlamanın yanı sıra hücrelerin çeşitlenmesine ve istenen dokuyu oluşturmasına yardımcı olmalıdır. Doku mühendisliğindeki en önemli konulardan birisi, gerekli yapay matrislerin ne şekilde tasarlanması ve sentezlenmesi gerektiğidir. Matris, hücrelerin rahatça beslenip oksijen almasına, hareket edip çoğalmalarına ve hücreler arası etkileşimin sağlanmasına yardımcı olmalı ve tedavi bittikten sonra doğal yollardan yok edilebilmelidir. Hücrelerin doğal yaşam ortamını oluşturan hücreler arası matristen gerekli olan bilgiler öğrenilmeli ve yapay matrisler için uygulanmalıdır. Doğal hücreler arası matris ile etkileşim halindeki birçok biyo-aktif molekül, hücrelerin yaşaması için çok önemlidir. Örneğin, kolajen ismindeki proteinler tutucu proteinler aracılığı ile hücrelere mekanik destek verirler. Hücrelerin üzerindeki integrin sınıfı proteinler de kolajenlere tutunmak için kullanılırlar. Doğal hücreler arası matris, içerisinde büyüme faktörleri de barındırır. Bazı büyüme faktörlerinin yardımı ile damar oluşumu sağlanarak hücrelere besin ve oksijen taşınması mümkün olur. Özet olarak yapay matrisler tasarlanırken birçok biyo-aktif molekülün doğru ve yerinde kullanılması gerekmektedir. Doku mühendisliğinde kullanılan matrisler bazı doğal veya sentetik malzemelerden yapılmaktadır. Bu matrisler en azından herhangi bir yan etkisi olmayan ve hücrelerin yaşamasına engel olmayan ve görevi bittikten sonra doğal yollardan uzaklaştırılabilen malzemeler olmalıdırlar. Doğal sistemlerden elde edilen matrislerden bir kısmı kolajen, kitozan ve glikozaminoglikenlerden oluşmaktadır. En çok kullanılan sentetik matrislerin başında da poli laktik asit, poli glikolik asit, poli kapralakton ve bir araya gelerek nanofiberler oluşturan moleküller gelmektedir. Doğal polimerler kolayca elde edilebilir olmasına rağmen, saflaştırma sonrasında içlerinde kalan hayvanlardan veya mikroorganizmalardan gelebilecek biyolojik kirlilik büyük tehlike oluşturmaktadır. Yapay polimerler, genelde kirlilikten kurtulmaya yardımcı olmakla beraber kimyasal tanımlanma, işlenebilirlik ve biyolojik aktiflik açılarından sorunludurlar. Matris üretiminde kullanılabilecek en ideal malzemelerden birisi bizim daha önce araştırmalarımızda geliştirdiğimiz programlanabilen moleküllerin oluşturduğu nanofiberlerdir. Bu çeşit malzeme kullanılarak yapılan matrisler biyolojik olarak aktif, zararsız ve tanımlanabilen küçük moleküllerden oluşmaktadır. Peptit içeren moleküller bir araya gelerek nanometre ölçeğinde kolajen nanofiberlerine benzeyen yapılar oluşturabilmektedir. Bu nanofiberler, üç boyutlu bir ortamda suyu hapsedebildikleri için hücrelerin yaşayabileceği uygun ortamlarda önemli biyoaktif molekülleri taşıyabilirler. Peptitlerden üretildikleri için de zamanla vücutta bulunan enzimler tarafından eritilirler.



Peptitler içeren nanoyapıların oluşturduğu ortam protein etkileşimleri için biyo-aktif gruplar ile tasarlanabilir ve iç bölümde bazı ilaçlar kontrollü salınım için taşınabilir. Farklı kimyasal ve biyolojik grupların bu nanoyapılar üzerinde kullanılabilmesi ile çok farklı doku mühendisliği uygulamaları mümkün olmaktadır. Biyo-aktif peptidik nanoyapıların omurilik felci tedavisinde bir farede sinir hücreleri geliştirilmesiyle ve bir tavşanın kulağındaki yaraların damarlaşma sağlanarak hızlı iyileştirilmesi için nasıl kullanıldıkları gösterilmektedir. Bu malzemelerin yakın zamanda ilaç olarak üretilebilmesi için gerekli klinik deneyler halen devam etmektedir. Doku mühendisliği, kanser tedavisinde de yardımcı olabilir. Kanserli dokuların cerrahi yöntemlerle uzaklaştırılmaları sonrasında oluşan boşluğun, aktif doğal doku ile doldurulması gerekmektedir. Şu andaki cerrahi tekniklerle vücudun bir bölgesinden diğer bölgesine doku nakli yapılması mümkün olsa da nakledilen dokunun beklenen görevleri yerine getirmesi zordur. Bu yüzden uzaklaştırılan dokunun yerine benzer bir doku üretme ihtiyacı vardır. Örneğin, cerrahi yöntemlerle alınan bir dil parçasının yerine herhangi bir deri dokusu yerleştirilmesi çare olamaz. Tat alma duygusunun tekrar gelişebilmesi için doğal dil dokusunun üretilmesine ihtiyaç vardır. Kök hücre çalışmalarında yapılan araştırmaların sonuçlarının ortaya çıkması ile doku mühendisliğinin uygulama alanlarının ne kadar geniş olduğu görülmektedir. Kök hücrelerinin birçok yeni doku ve organı üretmek için kullanılması planlanmaktadır. Özellikle tedavisi henüz mümkün olmayan felç ve kalp krizi gibi durumlarda yeni tedavi yöntemlerine ihtiyaç vardır. Kalp krizi geçiren hastaların kalbinde oluşan zararın tedavi edilmesi en önemli uygulamaların başında gelmektedir. Kalp hücrelerinin çoğalmayan hücreler olması kök hücrelerin kullanılmasını gerektirmektedir. Yeni üretilecek yapay matrisler, biyoaktif moleküller ve hücrelerin kullanılmasıyla, organ yetmezliği çeken hastaların kendi organlarının yeniden üretilmesi, yakın zamanda mümkün olacaktır. Hayat kalitesinin yükseltilmesi için bu tür biyoteknoloji çalışmaları büyük önem taşımaktadır. Kısa vadede doku mühendisliği çalışmalarıyla bulunacak çareler ile kemik kırıklarının, ciddi yanıkların, felçlerin, diyabetik hastaların ve kalp krizlerinin tedavisi gerçekleştirilebilecektir.

Kaynaklar

Ratner, Buddy D., Biomaterials Science-An Introduction to Materials in Medicine, Elsevier, 2004.

Lanza, Robert P., Robert S. Langer, William L. Chick, Principles of Tissue Engineering, Academic Press, 1997.

Hayvancılıkta Gen Çağı

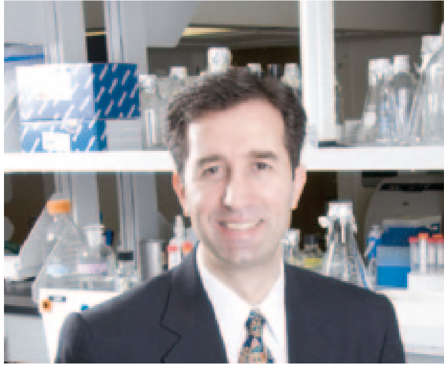
İnsanoğlu kalıtımın nasıl işlediğini bilmediği dönemlerde bile özelliklerin bir şekilde yeni nesillere aktarıldığının bilincindeydi. Bu bilinçle arzu ettiği özelliklere sahip hayvan ve bitkilere üreme şansı vererek bu özelliklere sahip olanların sayılarını artırdı. Yıllar süren gayretleri sonucu, seçilime dayalı yetiştiricilik olarak adlandırabileceğimiz bu metotla tarım ürünlerinin verimini olağanüstü düzeylere ulaştırmayı başardı. Geçtiğimiz Nisan ayında bir grup bilim insanı, çiftlik hayvanlarından sığırın gen haritasını çıkardıklarını bildirdi. Bu gelişme hayvancılıkta yepyeni bir çağa, gen çağına girişimizin de habercisi oldu. Bu bilgi sayesinde yüz yılı aşkın bir sürede elde edilen verim artışını belki on yıldan dahi kısa bir sürede gerçekleştirebilmek söz konusu olacak. Bu bilimsel ilerleme sayesinde çiftlik hayvanlarının seçimi artık onların ölçülen verimlerine göre değil, doğdukları anda genlerine bakılarak yapılacak. Hayvancılığın çok önemli olduğu ülkemiz için ise bu gelişme tarihi bir fırsat.

Anahtar Kavramlar

Bilim insanları ilk defa sığırın gen haritasını çıkardılar. Yüzyıldan fazla bir süredir eti ve sütü için özel olarak yetiştirilmiş sığırların gen haritalarını, onlar gibi özel seçime tabi tutulmamış düşük verimli yerli ırklarınki ile karşılaştırarak üstün et veya süt verimini hangi genlerin ve bu genlerin hangi dizilimlerinin belirlediğini öğrenmeye başladık.

Sığır gen haritası ile insan gen haritasının karşılaştırılması insan sağlığı için de önemli bilgiler sunuyor. Sığırların insanları çok etkileyen kanser ve otoimmün hastalıklara yakalanmama nedenlerinin genetik temellerinin belirlenmesi, insanlarda bu hastalıkların tedavisinde yönlendirici olacaktır.

Hayvancılığın çok önemli olduğu ülkemiz için bu gelişme tarihi bir fırsat; çünkü hayvanların verimlerine dayalı seçim sürecinden, daha doğar doğmaz genlerine bakarak verimlerini tahmin edeceğimiz bir sürece, hayvancılıkta gen çağına giriyoruz.



Bahri Karaçay, Iowa Üniversitesi Tıp Fakültesi Pediatri Bölümü, Çocuk Nörolojisi Kürsüsü öğretim üyesidir. Ayrıca aynı üniversitenin Gen Tedavi Merkezi ve Holden Kanser Merkezi üyesidir. Nörolojik doğum kusurları üzerinde genler düzeyinde araştırmalar yürütüyor. Beş yaşın altındaki çocuklarda görülen sinir sistemi tümörü nöroblastoma ve yine sinir sistemini etkileyen Alexander hastalığına gen tedavisi geliştiriyor. Ayrıca alkolün ve LCM virüsünün fetüs beyni üzerindeki etkilerini araştırıyor.

Yabani bitkilere ve av hayvanlarına dayalı yaşam tarzından yerleşik tarıma ve hayvancılığa geçiş, insanlık tarihinin en önemli değişim basamaklarından biridir. Evcilleştirilmiş çiftlik hayvanları ve bitki yetiştiriciliğiyle şekillenen ekonomiler bir yandan insan topluluklarının yeniden şekillenmesini sağlarken diğer yandan da hem coğrafyayı ve hem de biyoçeşitliliği etkiledi. Bu değişim zaman içerisine bütün dünyaya yayılınca etkileri sadece karayla sınırlı kalmadı, atmosferi de etkilemeye başladı.

Arkeolojik veriler hayvanların tarım amacıyla ilk defa yaklaşık 11.000 yıl önce, ülkemizin bir kısmını da içine alan Doğu Akdeniz ve Ortadoğu bölgelerinde evcilleştirildiğini gösteriyor. Bundan 100-150 yıl öncesine kadar, tarım ve hayvancılık binlerce yıl pek değişmeden uygulanageldi ve bu dönemde verimde çok az bir artış kaydedildi. Fakat özellikle Mendel'in çalışmalarıyla kalıtımın işleyişinin sayılara dökülmesi ve çoğu özelliğin gelecek nesillere ne oranda geçeceğinin matematiksel olarak hesaplanabileceğinin keşfi, tarım ve hayvancılıkta yepyeni bir devir başlattı. Yirmin-

ci yüzyılın başlarında arzu edilen özellikleri taşıyan çiftlik hayvanlarının yetiştirilmesiyle ilerleme de hızlandı. Son yirmi yılda gen bilimlerinde elde edilen ilerlemelerin bu gelişimi daha da hızlandıracağı kesin.

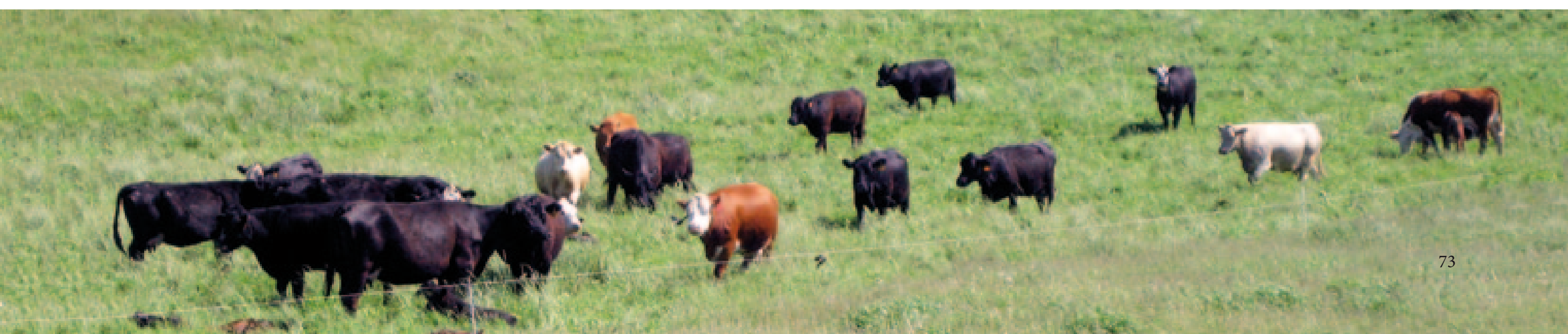
Bu konudaki önemli gelişmelerden biri *Science* dergisinin 24 Nisan sayısında yayımlanan bir makaleyle bütün dünyaya duyuruldu. Yirmi beş farklı ülkeden yaklaşık üç yüz araştırmacının katkılarıyla gerçekleştirilen bu çalışmada bir sığırın gen haritası çıkarıldı. Yine aynı dergide yayımlanan bir başka çalışmada ise değişik sığır ırkları arasında genler düzeyinde karşılaştırma yapılarak aralarındaki benzerlik ve farklılıkların belirlendiği duyuruluyordu. Elde edilen bilgiler sadece hayvansal üretim için değil biyolojik bilimler açısından da son derece önemli. Çünkü bu ve benzeri projeler sayesinde örneğin bir sığırı neyin et sığırı veya neyin süt sığırı yaptığını veya bir koyunu neyin koyun yaptığını veya bir insanı diğer türlerden ayıran genetik farklılıkların neler olduğunu öğrenmeye başladık. Örneğin, çıkarılan gen haritası, sığırların 22.000 civarında gene sahip olduğunu gösterdi. Bu sayı insanın sahip olduğu gen sayısına çok yakın. Ayrıca sığırların çok sayıda geninin insanlarınkilere çok benzediği ve hatta bazılarının tamamen aynı olduğu keşfedildi. Bu benzerlik ve farklılıklar insan sağlığı için son derece önemli. Çünkü belli hastalıklar açısından türler arasındaki farklılıklar ve bu farklılıkların genetik temelleri, insan hastalıkları hakkında önemli ipuçları verecektir. Örneğin, büyükbaş hayvanların kansere çok nadiren yakalandıkları bilinen bir gerçektir. Ayrıca büyükbaş hayvanlarda, otoimmün hastalıklar adını verdiğimiz ve bağışıklık sisteminin kendi vücudunu yabancı olarak algılayıp ona saldırarak dokularını zedelemesi şeklinde gerçekleşen hastalıklar da pek görülmüyor. İnsanlarda ise bu hastalıklar önemli bir hastalık grubunu teşkil ediyor. Sığır ve insan gen haritasının bağışıklık sistemiyle ilgili kısımlarının karşılaştırılması hangi genlerin onları örneğin otoimmün hastalıklara karşı dayanıklı kıldığını gösterecektir. Bu bilgi daha sonra insan hastalıklarının tedavisinde yol gösterici olacaktır. Aklınıza şöyle bir soru gelebilir: Zaten laboratuvar hayvanları ile bu soruların cevabını aramaya çalışmıyor muyuz? Fare ve kobaylarla bu sorulara cevaplar aradığımız doğru, ancak bu türlerle insanlar arasındaki genetik farklılıklar, bazen elde edilen sonuçların insanlara uygulanmasını engelliyor. Genetik açıdan insana çok daha yakın olan büyükbaş hayvanlardan elde edilecek sonuçların insanlara uygulanması bu sorunu da ortadan kaldırabilecektir.



Keith Weller / USDA

Holstein ırkı, süt üretimi için geliştirilmiş sığır ırklarından biridir ve dünya genelinde en yaygın sığır ırklarındandır.

Science dergisinin aynı sayısında yer verilen ikinci bir çalışmada, araştırmacılar bir et sığırının gen haritasını çıkardıktan sonra bunu yirmi bir farklı sığır ırkının gen dizilimleriyle karşılaştırdılar. Bu çalışma ırklar arasındaki benzerlikleri gösterdiği gibi farklılıkları da ortaya çıkardı. Sonuçlar yüzlerce yıldır yapılan seçilime rağmen değişik sığır ırkları arasında hâlâ önemli düzeyde genetik çeşitlilik olduğunu ve bu çeşitliliğin en azından insanlar arasında görülene denk düzeyde olduğunu gösterdi. Bu gerçek de sadece belli özellikleri taşıyan büyükbaş hayvanların yetiştirilmesi sonucu genetik çeşitliliğin daralmış olacağı ve sonuçta sığır ırkının devamlılığının tehlikeye gireceği savını çürütmüş oldu. Herhangi bir türde genetik çeşitliliğin ortadan kalkması, o türü hedef alan bir tehlikeye karşı türün bütün üyelerini savunmasız kılacağı için türün devamlılığını tehdit edecektir. Örneğin, öldürücü bir virüs salgını türün bütün fertlerinin ölümüne ve türün ortadan kalkmasına neden olabilir. Buna karşılık eğer türde yeterli düzeyde genetik çeşitlilik varsa, türün bazı üye-



Kültür ırkı olarak adlandırdığımız ırklar, yüz yıla yakın bir süredir üstün verimleri dolayısıyla seçilen hayvanlardan oluşurlar.

Fotoğraf: Bahri Karaçay



Visual Photos

Üstün verimli et ve süt sığırlarının sayısını artırmanın bir yolu da onları klonlamaktır. Önce klonu yapılacak sığırın kulağından küçük bir doku parçası alınır ve laboratuvarda hücrelerine ayrıştırılır. Bu hücreler çekirdeği çıkarılmış sığır yumurta hücreleri ile kaynaştırılır. Verilen küçük bir elektrik akımı ile bölünme başlatılır. Bu şekilde elde edilen embriyolar taşıyıcı ineklerin rahimlerine aktarılır. Doğan buzağılar genetik olarak hücrelerin elde edildiği sığırın kopyalarıdır. Aynı ortam ve beslenme koşullarında onlar da üstün verimli olurlar.

leri virüse karşı dayanıklı çıkacak ve bir kısmı ortadan kalksa bile geride kalanlar türün devamlılığını sağlayacaktır. Farklı sığır ırklarının genomlarında görülen genetik zenginlik, değişik nedenlerle bazı ırklar ortadan kalksa bile geride yeterli sayıda sığır ırkının kalacağını gösteriyor.

Klasik anlamda yapılan büyükbaş hayvan yetiştiriciliğinde, sürüyü oluşturan hayvanların ferdi verimleri kayda geçirilir ve verimi en yüksek olanlar damızlık olarak kullanılır. Bu şekilde uygulanan seçilimle zaman içerisinde verimde önemli artışlar sağlandı. Geçtiğimiz yüzyılın başlarında suni tohumlama tekniğinin ilk defa başarıyla uygulanması, hayvan ıslahında yeni bir dönem başlattı. Suni tohumlamanın yaygın olarak kullanılmaya başlandığı 1940'lı yıllardan itibaren üstün verimli boğaların spermleri okyanus ötesi ülkelere dahi taşınarak üstün verimli hayvanların sayısı kısa sürede artırıldı. Ülkemizde de suni tohumlama uygulamaları her geçen gün daha da yaygın hale geliyor.

Bununla beraber klasik yöntem uzun zaman alır. Suni tohumlama veya damızlıkta kullanılacak boğaların seçimi en az dört beş yıl sürer. Örneğin süt sığırı sürüsünün oluşturulmasında kullanılacak boğaların seçiminde önce adayların farklı ineklerden doğan dişi yavrularının süt verimleri yaklaşık beş yıl süreyle takip edilir ve kayıtlara geçilir. Elde edilen rakamlar karşılaştırılır ve denenen boğalardan hangilerinin daha yüksek süt verimli yavruları olduğu belirlenir. Diğerlerinden üstün olan boğalar, sürünün devamlılığını sağlamak üzere damızlıkta kullanılır. Üreticiler bu "seçilim yöntemi"ni çiftlik hayvanlarına uygulayarak değişik özelliklere sahip onlarca hayvan ırkı geliştirdiler. Bugün eti için yetiştirilen et sığırları olduğu gibi süt verimi yüksek olan süt sığırları da yetiştiriliyor. Sığır gen haritasının çıkarılması, değişik özellikleri için yetiştirilen ırklarda bu özelliklerin hangi gen dizilimleri tarafından belirlendiğini de ortaya çıkarmaya başladı. Yakın bir gelecekte, örneğin üstün bir et verimi sağlayacak genetik dizilimlerin neler olduğu veya üstün bir süt verimini sağlayacak genetik dizilimlerin neler olduğu belirlenerek her yeni doğan buzağıda bu dizilimlerin varlığına bakılacaktır. ABD'de daha şimdiden bu düşünceyle yola çıkıp çiftlik hayvanlarına genetik testler yapan şirketler bulunuyor. Doğan buzağıların kuyruklarından alınan kıl örnekleri postayla bu şirketlere gönderiliyor, şirketin laboratuvarında kıl örneklerinden DNA izole edilerek sınırlı sayıdaki genin üstün özellik sağlayan dizilimlere sahip olup olmadığına bakılıyor. Yetiştiriciye gönderilen genetik kapasite raporunda, buzağının gelecekteki veriminin tahmini yer alıyor. Fakat şimdilik bu testlerde bakılan gen sayısı çok sınırlı. Sığır gen haritasının tamamlanması bu tür testlerle sadece birkaç gene değil, bir anda yüzlerce veya binlerce gene bakmayı mümkün kılacak. Yakın bir gelecekte ülkemizde de genlere bağlı hayvancılığın başlayacağı şüphesiz. Genom hayvancılığı hem yerli ırklarımızdan üstün verimli et sığırı veya süt sığırı tiplerinin elde edilmesini sağlayacak, hem de ülkemizde yetiştirilen kültür ırklarının verimlerinin daha üst düzeylere taşınmasına imkân verecektir.

Moleküler yaşam bilimlerindeki gelişmeler, hayvan yetiştiricilerine bahsettiğimiz gen veya genom hayvancılığı devrini yaşatması yanında, hayvancılığı yepyeni ufuklara da taşıyacaktır. Şimdi et sığırcılığında önemli olan, etin kalite ve miktarını etkileyen bir gen örneğinde hayvancılıkta gen çağının nasıl bir gelecek vaat ettiğine bir göz atalım.

Modern anlamda sığır yetiştiriciliği dendiğinde akla gelen ilk ülke genellikle Belçika değil, İngiltere veya Hollanda olur. Bunda Belçikalı çiftçilerin geniş mera ve otlak alanlarına sahip olmayışlarının önemli bir etkisi olsa gerek. Belki de bu gerçek, onları ellerindekiyle daha fazlayı başarabilmenin yollarını aramaya itti. Bu gayretlerinde ithal edilen etlerin daha ucuz olmasının yanında kendi üretim maliyetlerinin yüksek olmasının da önemli etkisi oldu. Çiftçilerin bu ekonomik zorlukları aşma gayretleri yeni bir sığır ırkının geliştirilmesini sağladı. Belçikalı çiftçiler özellikle son kırk yıllık gayretleri sonucu "Belçika Mavisi" adı verilen bir et sığırı ırkı geliştirdiler.

Belçika Mavisi, diğer sığırlarla aynı ortamı paylaşıp aynı ot ve yemleri tüketmesine rağmen diğerlerinden % 20 daha fazla kas yapıyor. Bu ırkı fuarlarda ilk kez gören yetiştiriciler aralarında "Arnold

Schwarzenegger geni taşıyor olmalı" esprisini yapmaktan kendilerini alamıyorlar. Çünkü "çifte kaslı" olarak da adlandırılan Belçika Mavisi'nin kaslarını uzaktan dahi fark etmemek imkânsız. Olağanüstü düzeyde kas oluşumu bazen onların rahatlıkla yürümelerini engelleyecek düzeye ulaşır. Ağırlıkları bir tona yaklaşabilir. Ayrıca buzağıları çok büyük olduğu için doğumlar sezaryenle gerçekleştirilir.

Belçikalı çiftçiler çifte kaslı sığırları aslında 1807 yılından beri biliyorlardı; ancak dikkatlerini bu özelliğe çevirmeleri 1950'li yılları buldu. Belçika Mavisi'ni gören genetikçi veya moleküler biyolog bilim insanlarının düşündüğü ise, yıllar süren ıslah çalışmalarıyla bu hayvanlarda kas oluşumundan veya gelişiminden sorumlu genlerden bir veya birkaçında birtakım farklılıkların ortaya çıkmış olması gerektiğiydi; bu değişikliğin ne olduğu bulunmalıydı. Nitekim bu düşüncelerle yola çıkan biri Belçika'da, diğer ikisi ABD'de olan üç farklı araştırma grubu birbirlerinden bağımsız olarak büyük gayret ve uzun süren çalışmalar sonucunda Belçika Mavisi'nin çifte kaslı olmasının nedenini buldular. Belçika'nın Liege Üniversitesi'nden Michael Georges'in önderliğindeki grup, 1997 yılında *Nature Genetics* dergisinde yayımladıkları bir makaleyle Belçika Mavisi ırkının "miyostatin" adı verilen bir gende mutasyon taşıdığını bildirdiler.

Grubun çalışmaları 1980'lerde başlamıştı. Çifte kaslılığa neden olan genin bulunmasının hayvancılık için çok önemli olduğu barizdi. Georges ve grubu o günlerin bilgi ve teknolojisiyle çifte kaslılığa neden olan mutasyonun sığırların iki numaralı kromozomu üzerinde olduğunu buldular ve bu bulgularını 1995 yılında bilim dünyasına duyurdular. Ancak iki numaralı kromozomda yüzlerce gen vardı ve hangisinin çifte kaslılık geni olduğunu bulmak için daha çok çalışmaları gerekiyordu. Bu konuda önemli bir gelişme, farklı bir tür üzerinde yapılan bir çalışmadan elde edildi. Johns Hopkins Üniversitesi'nden Se-Jin Lee ve lisansüstü öğrencisi Alexandra McPherron farede miyostatin adı verilen bir genin, kas gelişmesini kontrol ettiğini ve normal sınıra ulaştığında kas gelişimini durdurduğunu buldular. Farede miyostatin genini mutasyona uğrattıklarında mutasyonu taşıyan fareler, normal farelerin iki hatta üç katı büyüklüğe ulaştılar. Lee ve McPherron'un bulgularını yayımlamaları çifte kaslı Belçika Mavisi sığırı üzerinde çalışan bilim insanları arasında da bir yarış başlattı. Georges ve grubu önce fare geninin diziliminden yola çıkarak insan miyostatin geninin dizilimini belirledi ve kromozom üzerindeki yerini buldu. Bu bilgiyi ve insan ile sığır DNA'sı arasındaki benzerlikleri kullanarak sığırdaki çifte kaslılık geninin yerini kolaylıkla buldular. Bu bilgiyi elde ettikten sonra miyostatin genini hem normal sığırlardan ve hem de çifte kaslı sığırlardan elde edip onların DNA dizilimlerini karşılaştırdılar. Çifte kaslı sığırların miyostatin geninde bir mutasyon taşıdığını buldular. Bu mutasyon miyostatin proteininin sentezini çok erken sonlandırıyor ve dolayısıyla onu işlemez hale getiriyor. Normal miyostatin proteini olmayınca kas gelişiminin kontrolü de ortadan kalkıyor. Aynı stratejiyi uygulayan Lee ve grubu, Georges ve grubunun bulgularının aynısına ulaşıp onların verilerini teyit ettiler, Belçika Mavisi sığırındaki çifte kas geni miyostatin idi.



Belgimex

Belçika Mavisi sığır ırkı miyostatin adı verilen ve kas gelişmesinin normal sınırlarda kalmasını kontrol eden geninde mutasyon taşıyor. Mutasyon sonucu bu sığırlar normalden çok daha fazla kas yaparlar. Bu özelliklerinden dolayı Belçika Mavisi'ne "çifte kaslı" da denir.

Miyostatin genindeki mutasyon, kas miktarını artırırken etin kalitesini değiştirmiyor; çünkü mutasyonun sonucunda kastaki lif sayısı artıyor. Eğer kas miktarındaki artış kas liflerinin sayısından değil de liflerin kalınlığındaki artıştan dolayı olsaydı, o zaman etin kalitesi azalacaktı. Çünkü lif kalınlığının artması ile etin gevrekliğinde azalma olur. Sadece miyostatin geni ile ilgili bu bilgilere sahip olduktan sonra ülkemiz hayvancılığına bunu nasıl uygulayabileceğimizi farklı senaryolarla inceleyelim. Vereceğimiz bu örnek (özellikle gen yapısının değiştirilmesi) aslında ekonomik açıdan önemli özellikleri kodlayan genler için de geçerli olacaktır. Ancak pek çok özelliğin tek bir gen tarafından değil çok sayıda genin çalışması ile ortaya çıktığını belirtmem gerekiyor. Çok sayıda genin etkilediği özellikler için yukarıda belirttiğimiz genetik tarama metodunun uygulanması çok daha kolay olacaktır. Miyostatin geni ile ilgili olarak akla ilk gelen senaryo şu, madem bu hayvanlar Belçika'da yetiştiriliyor, o zaman ithal ederek ve onları yetiş-

tirerek ülkemizde et sığırcılığının ilerlemesini sağlayamaz mıyız? Her ne kadar mantıklı ve kısa sürede sonuç verecek bir strateji gibi görünse de ülkemizin koşulları göz önüne alındığında bu yolu seçmenin sorun çıkaracağı görülür. Ülkemizde et sığırcılığının en fazla yapıldığı yer olan Doğu Anadolu bölgesinin iklimi ve coğrafyası, hayvan yetiştiriciliğinde uygulanan bakım ve beslenme tarzı, Belçika Mavisi'nin alışık olduğu ılıman iklim, mera ve otlak arazileri ile bakım ve beslenme tarzından çok farklıdır. Nitekim geçmişte sığırcılığın geliştirilmesi için ithal edilen kültür ırklarından İsviçre Esmeri, Doğu Anadolu'nun sert iklimine ve coğrafyasına, beslenme tarzına ve hayvan sağlığı hizmetlerinin yetersizliğine uyum sağlayamamış ve bu nedenle ırk bölgede sınırlı düzeyde yayılabilmiştir. Bununla beraber Ege ve Trakya bölgelerimizin ikliminin ve coğrafik özelliklerinin, hayvan yetiştirme uygulamalarının Doğu Anadolu'ya kıyasla Avrupa ülkelerine çok daha yakın olması, Belçika Mavisi'nin ithal edilerek bu bölgelerde başarıyla yetiştirilebilmesi olasılığını artırıyor.

İkinci senaryo ise Belçika Mavisi boğaların veya spermlerinin, yerli sığır ırklarımızın tohumlanmasında kullanılması ve bu yolla çifte kaslılık özelliğini taşıyan melez bir sığırın üretilmesidir. Yine geçmiş tecrübelere dayanarak bu yolun da sorunlu olacağını söyleyebiliriz. Belçika Mavisi ırkının aşırı kaslı olmasının buzağıların doğumunu zorlaştırdığını ve bu nedenle doğumların sezaryenle yapılmak zorunda kalındığını belirtmiştim. Nitekim bu sorun, hayvancılığının temelini binlerce hayvanı barındıran büyük işletmelerin oluşturduğu ABD'de Belçika sığırının yayılmasını önlemiştir. Kültür ırkları ile karşılaştırıldığında yerli ırklarımız çok daha küçük olduğu için, kültür ırkları ile yerli ırklarımız arasındaki melezlemelerde doğum zorluğu en önemli sorunlardan biri olmuştur. Veterinerlik hizmetlerinin yetersiz olduğu kırsal bölgelerimizde çiftçilerimiz doğum zorluğu nedeniyle çok sayıda hayvanı doğum sırasında kaybetmişlerdir.

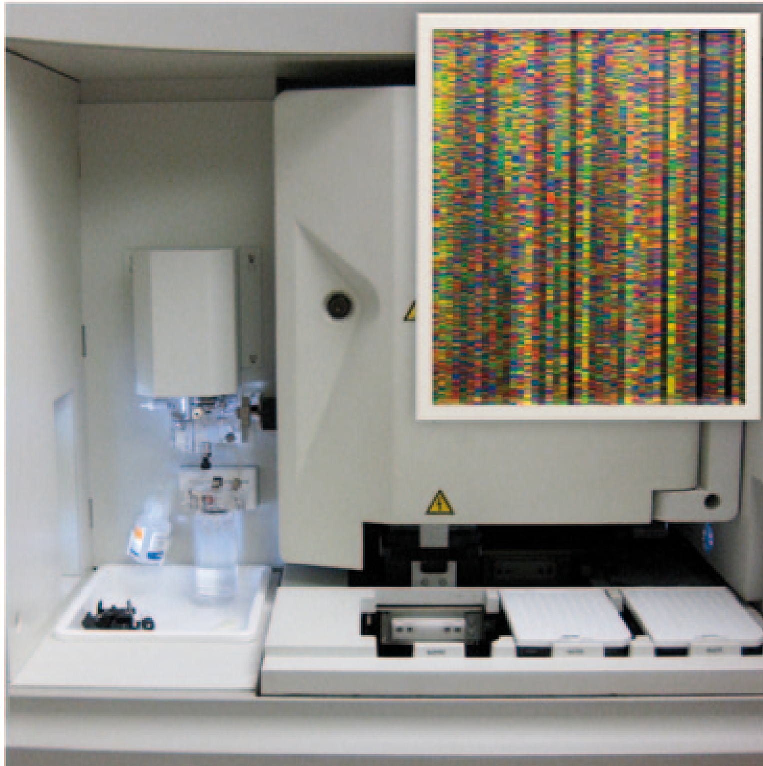
Kültür ırkları, yüksek verimli olmalarının yanında iklime, çevresel koşullara ve hastalıklara karşı daha hassas olmalarıyla bilinirler. Yerli ırklarımız ise düşük verimlidirler fakat kötü iklime ve çevresel koşullara, özellikle hastalıklara karşı kültür ırklarından çok daha dayanıklıdırlar. O halde yerli ırklarımızın et verimlerini, örneğin miyostatin geninin yapısını bozarak artıramaz mıyız? Veya bir şekilde miyostatin geninin çalışmasını engelleyerek aynı sonuca ulaşamaz mıyız? Böylece iç, doğu ve güneydoğu Anadolu'nun şartlarına binlerce yıl içinde uyum sağlamış yerli ırklarımızın genetik potansiyellerini artırabilir miyiz?

Genetik alanında DNA'nın yapısının keşfinden Dolly'nin klonlanmasına kadar geçen süredeki gelişmelere bakıldığında, bilimsel ve teknolojik açıdan böyle bir senaryoyu gerçekleştirecek seviyeye ulaşmış olduğumuz söylenebilir. Ayrıca iki alternatif bile söz konusu: miyostatin geninin çalışmasını farmakolojik olarak yani ilaçlarla engellemek veya yerli ırklarımızın miyostatin geninin yapısını bozmak (mutasyon yaratılması).

Miyostatin geninin kas gelişimindeki rolünün belirlenmesinin ardından Avrupa ve ABD'deki ilaç şirketlerinin pek çoğu, bu proteinin çalışmasını önleyecek ilaçlar geliştirmek üzere araştırmalar başlattılar. İlk girişimler sırasında hayvancılıktaki uygulamalar düşünülmüştü. Fakat daha sonra geliştirilecek böyle bir ilacın insan sağlığı açısından ne kadar yararlı olacağının anlaşılmasıyla çalışmalar insanlara yönlendirildi.

Yaşamın doğal bir parçası olarak 30 ile 80'li yaşlar arasında, kaslarımızın yaklaşık olarak üçte birini kaybediyoruz. Bu kayıp ileri yaşlarda kas gücünün giderek azalmasına, gençlikte yapılabilen pek çok fiziksel aktivitenin artık yapılamamasına neden olur. Bir de Duchanne kas distrofisi gibi, kasların normalden çok daha hızlı bir şekilde za-

Bilim insanları farklı ırkların gen dizilimlerini ileri teknolojiye sahip dizilim aletleriyle belirleyerek et ve süt verimi için önemli olan genleri belirliyorlar. Aşağıda Foto Gen dizilim belirleme makinesi ve çıktısı görülüyor.



Bahri Karaçay

yıflaması ve kaybolması (kas hücrelerinin ölmesi) ile sonuçlanan hastalıklar vardır. Miyostatin geninin çalışmasının önlenmesi ilk bakışta vücutta daha fazla kas oluşmasını sağlayarak yukarıdaki sorunlara çözüm olacak gibi görünüyor. Bu amaçla yola çıkan ilaç şirketleri, miyostatin proteininin çalışmasını önleyecek ilaçlar geliştiriyorlar. Stratejilerden biri, miyostatin proteinine karşı antikor üreterek vücuda giren örneğin bakteri proteinlerinin bağışıklık sistemimiz tarafından yok edilmesine benzer bir şekilde miyostatin proteininin parçalanmasını sağlamaktır. Geliştirildiği takdirde bu tür ilaçlar kullanılarak sığırlarda et verimi artırılabilecektir. Ancak bunun için geliştirilen ilaçların et sığırlarına belirli aralıklarla verilmesi gerekecektir. Tüketicinin bu şekilde ilaçla beslenen hayvanlardan elde edilen ürünlere genelde olumsuz yaklaşımı büyük ihtimalle böyle bir uygulamayı sınırlandıracaktır.

Yerli ırklarımızın et verimlerini onların miyostatin genlerinin yapısını bozarak artıramaz mıyız? 1996 yılında Dolly'nin klonlanması, memeli hayvanların genetik yapılarında değişiklik yapılabileceğinin de müjdecisiydi. Bilim insanları tek bir hücre ile başlayıp onun genetik yapısını istedikleri yönde değiştirdikten sonra çekirdek transferi ile bu hücreden tam bir canlı elde etmeyi başardılar (Bakınız Karaçay, B., *Bilim ve Teknik* Sayı 496, s. 52-57, 2009). Aynı teknik uygulanarak yerli ırkların miyostatin geni ile oynanarak et verimleri artırılabilecektir. Bunun için önce, örneğin Doğu Anadolu Kırmızısı ırkından üstün verimli bir boğa seçilir. Bu boğanın derisinden alınacak küçük bir doku parçası laboratuvar şartlarında hücrelerine ayrıştırılır ve sonra bu hücreler uygun besi ortamlarında büyütülür. Yerli ırka ait miyostatin geni hemen her moleküler biyoloji laboratuvarında bulunan ve rutin olarak kullanılan PCR adını verdiğimiz bir teknikle izole edilir. Bu gende Belçika Mavisi'nde görülen mutasyon yaratılır ve deriden elde edilen hücrelere aktarılır. Bu hücrelerden bazılarında, aktarılan gen ile hücrenin kendi miyostatin geni arasında parça değişimi gerçekleşecektir (homolog rekombinasyon adı verilen bu mekanizmayı keşfeden Mario Capecchi 2007 yılı fizyoloji ve tıp dalında Nobel aldı). Parça değişimi sonucu mutasyon hücrenin DNA'sına yerleşecektir. Bu hücrenin çekirdeği çıkarılır ve aynı ırkın ineklerinden elde edilip çekirdeği çıkarılmış yumurta hücresine aktarılır. Böylece ortaya çıkan yumurta hücresinin çekirdeği, mutasyonlu miyostatin geni taşıyor olacaktır. Çekirdek transferi yapılmış bu yumurta hücresine küçük bir elektrik akımı verilerek bölünmeye başlaması sağlanır. Birkaç bölünme geçirdikten sonra bu hücre yumağı (embriyon) taşıyıcı bir ineğin rahmine aktarılır. Embriyon transferi et ve süt sığırcılığında yaygın olarak kullanılır. Sığırda gebelik süresi ortalama 282 gündür. Bu süre sonunda doğacak buzağının bütün hücreleri miyostatin geninde mutasyon taşıyacak ve büyüdüğünde çifte kaslı bir inek veya boğa olacaktır. Böyle bir buzağı büyüyüp boğa olunca onun spermi kullanılarak birkaç yıl içerisinde Doğu Anadolu Kırmızısı olan fakat çifte kaslı çok sayıda et sığırı üretilebilecektir.

Genom hayvancılığının sadece büyükbaş hayvan üretiminde değil, diğer çiftlik hayvanlarının üretiminde de kullanılması kısa bir süre içinde var olan ırklardan üstün verimli sürülerin elde edilmesini sağlayacaktır. Genom hayvancılığı ile bir yandan kültür ırkı hayvanların verimlerinde artış sağlanırken, diğer yandan asırlar boyu herhangi bir seçilime tabi tutulmamış fakat genetik zenginliği nedeniyle üstün verimli hayvanların elde edileceği kesin olan yerli ırklarımızdan sadece eti, sadece sütü veya sadece yapağısı için yetiştirilecek özelleşmiş alt ırkların elde edileceği günler de gelecektir. Genom hayvancılığında doğan her hayvanın genetik kapasitesi yaşamının ilk birkaç gününde belirleneceği için, yerküremizin giderek azalan kaynakları da en etkin bir şekilde kullanılmış olacaktır.


Bahri Karaçay

Yüzyılı aşkın bir süredir yapılan seçilim uygulamaları özellikle et verimi geliştirilmiş sığır ırklarını ortaya çıkardı.

Kaynaklar

The Bovine Genome Sequencing and Analysis Consortium, Elsik, C. G., Tellam, R. L., Worley, K. C., "The Genome Sequence of Taurine Cattle: A Window to Ruminant Biology and Evolution", *Science*, Cilt 324, Sayı 5926, s. 522, 2009.

The Bovine HapMap Consortium, "Genome-Wide Survey of SNP Variation Uncovers the Genetic Structure of Cattle Breeds", *Science*, Cilt 324, Sayı 5926, s. 528-532, 2009.

Fredericks, R., Lewin, H., Worley, K., Palmarini, M., *Science* Magazine Podcast Transcript, Cilt 324, Sayı 5926, 2009. http://www.sciencemag.org/cgi/data/324/5926/537-b/DC1/1

Lewin, H. A., "It's a Bull's Market", *Science*, Cilt 324, Sayı 5926, s. 478, 2009.

Grobet L. ve ark., "A deletion in the bovine myostatin gene causes the double-muscled phenotype in cattle" *Nature Genetics*, Cilt 17, Sayı 1, s. 71-74, 1997.

Şebnem Elbek

Jeofizik Mühendisliği Bölümü,
Onsekiz Mart Üniversitesi,
Çanakkale

Adli Araştırmalarda Yeni bir Pencere Adli Jeofizik

Ekibin tecrübeli lideri dedektif Mac Taylor'a göre
"New York'ta herkes yalan söyleyebilir; ama kanıtların yalan söylediği çok nadirdir."
Kanıt Peşinde (*Crime Scene Investigators*)


JUPITERIMAGES

Bir cinayetin aydınlatılmasından savaş suçlarının araştırılmasına kadar adli konularda yeni yöntem arayışları, 1970'lerden günümüze değin jeoloji, jeofizik ve botanik biliminde de araştırmalar yapılmasına yol açtı. 18. yüzyılın sonları ve 19. yüzyılın başlarında adli bilimler alanında hızlı gelişmeler oldu. Bu dönemde mikroskobik, fotografik ve radyolojik kimi yöntemlerden yararlanılmaya başlandığı görülüyor. 1891'de Sir Arthur Conan Doyle'un yazdığı Sherlock Holmes serisi, 1909 yılında Rodolphe Reis'in kurduğu Lousanne Üniversitesi'ndeki Adli Bilimler ve Kriminoloji Fakültesi, 1910 yılında Locard'ın Lyons'da (Fransa) kurduğu kendine ait kriminal laboratuvar ve özellikle 2. Dünya Savaşı sonrası aslında savaşta kullanılmak üzere geliştirilen teknik ekipman ve yöntemlerin bilimsel amaçlarla kullanılması gibi örnekler, adli bilimlerde yerbilimleri uygulamalarının gelişimi açısından önem taşır.

Bilimsel olarak yürütülen suç araştırmalarını en iyi belgelendirmiş kişilerden biri olan Hans Gross yazdığı kitapta adli tıp, toksikoloji, seroloji (adli biyoloji ve DNA), balistik ve adli jeoloji gibi konular üzerinde durmuş, bir ayakkabıdan alınan toprak ve benzeri materyalden yola çıkarak (petrografik çalışma) işlenen suçun araştırılması gibi incelemelere değinmiştir. Adli bilimlerde yerbilimsel araştırmaların suçlu tanımlama açısından başlangıcı 100 yıl önce Alman yerbilimci Georg Popp'un yaptığı çalışmalara dayanır. Georg Popp, Kasım 1904'te bir suçun aydınlatılması için kendisine başvurulduğunda, delil olarak olay yerinden topladığı mineral tanelerini olayın aydınlatılmasında kullanmış. Terzilik yapan Eva Disch adlı bir kadın, tarlada kendi eşarbıyla boğulmuş olarak bulunmuş. Popp olay yerinde yaptığı araştırmada, kirli bir mendil üzerinde burun silinmesiyle mendile bulaşan kömür ve enfiye parçacıklarında hornblent mineral taneleri tespit etmiş. Gaz istasyonunda kömür yakan, ayrıca yarı zamanlı olarak da yerel çakıl madeninde çalışan Karl Laubach bir numaralı cinayet zanlısıymış. Popp, zanlının tırnaklarında kömür, enfi-



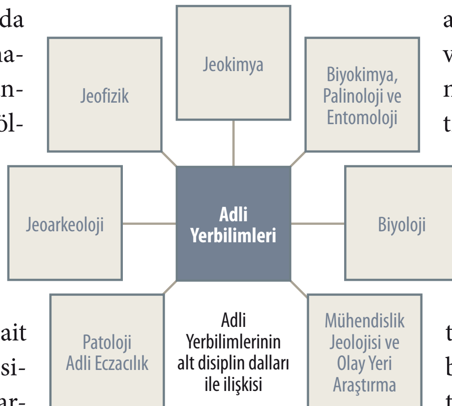
ye ve hornblent minerali tespit etmiş, ayrıca zanlının pantolonuna bulaşan toprak parçalarını öldürülen kadının vücudunda ve Karl Laubach'ın eviyle olay yeri arasında da görmüş. Suçlunun cinayeti işlediğini itiraf etmesi, Popp'un Mikroskop Dedektifi olarak ünlenmesine yol açmış. 1908 yılında gündeme gelen Margarethe Filbert davasıyla Popp, adli olaylarda jeolojik incelemelerden yararlanmayı genel bir yapıya oturtmuş.

Adli araştırmalarda yalnızca günümüze ait olaylar incelenmez. Her ne kadar çalışmaları tam anlamıyla adli yerbilimsel içerikli olmasa da, McCrone'un çalışmalarına değinmeden geçmemek gerek. Tarihsel birtakım kuramları sınamak düşüncesiyle mikroskobu geliştiren Walter C. McCrone'un araştırmaları arasında en ilginç olanı Napoléon Bonaparte'a (1769-1821) ait saç örneklerini inceleyerek ölüm nedenini araştırmasıdır. Tarihsel kayıtlarda Napoléon'un tekrar tahta çıkmasını engellemek için gardiyanlar tarafından zehirlenerek öldürüldüğü şüphesi egemenken, McCrone'un incelediği saç örneğinde arsenik seviyesi çok düşük çıkmıştır.

McCrone'un bir diğer çalışmasıysa Beethoven'a ait saç örneğininin incelenmesidir. Beethoven'ın 1826'da kardeşi Karl ile birlikte Gneixendorf'ta yaptığı tatilin ardından Viyana'ya dönüşünde, çok ilerlemiş siroz nedeniyle 26 Mart 1827'de öldüğü biliniyor. McCrone, saç örneği üzerinde yaptığı analizde, ölmeden önce ünlü müzisyenin vücudunda yüksek oranda kurşun bulunduğunu, yani Beethoven'ın kurşun zehirlenmesine uğradığını saptamış.

Adli Araştırmalarda Jeofizik

Günümüzde yerbilimleri, özellikle cinayet yerinin ve suçlunun kimliğinin belirlenmesinde delil elde etme açısından, etkin bir rol oynuyor. Bir cinayetin ardından, mağdurun bulunamaması ve/veya suçlunun kimliğinin belirlenememesi durumunda (terör sonucu toplu ölümler ve deprem, sel gibi felaketler sırasında insanların kaybolması da bu bağlamda değerlendirilebilir), temelde adli yerbilimleri, jeoloji, jeofizik ve geniş ölçüde çevre bilimlerini içeren mahkeme öncesi araştırma yöntemlerine başvurulur. Adli yerbilimlerinin sınırları tam olarak tanımlanamamakla birlikte çalışma alanı birçok disiplinle çakışır. Adli yerbilimleri kayaç, sediment, toprak, hava, su, doğal olaylar ve bunların süreçlerini ve etkilerini tüm yönleriyle inceler.

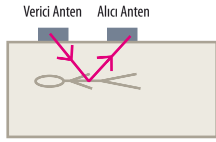


Adli Yerbilimlerinin alt disiplin dalları ile ilişkisi

20. yüzyılın ilk yarısında İsviçre, Fransa, Almanya, İngiltere ve ABD'deki hükümetlere bağlı birimler ve eğitim kuruluşları, araştırma laboratuvarları aracılığıyla adli bilimlerde jeolojik uygulamaları destekleyerek geliştirmiş. 1973 yılı başlarında A.V. Alongi'nin yeraltına gömülmüş bir köpeğin yerini "yer radarı" kullanarak belirlemesi, jeofizik çalışmalarının adli araştırmalara katkısı konusunu gündeme getirdi. 1975 yılında Raymond Murray ve John Tedrow tarafından yayımlanan Adli Jeoloji adlı kitap, adli yerbilimleri tekniklerini anlatması bakımından bir mihenk taşı olarak kabul edilir.


Visual Photos

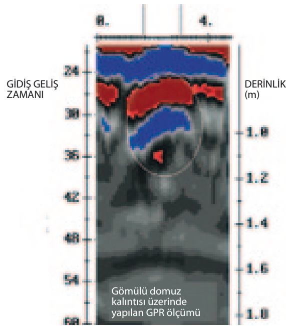
Herhangi bir "adli olayın" ne şekilde gerçekleştiğini, yani olayın oluş şeklini ve nedenini araştırmak, suçluya ve mağdura ilişkin suç kanıtlarının saptanması, olaydan kaynaklanan zarar ve kaybın belirlenmesi için olay yerinde yapılan adli işlemlere "keşif" ya da "olay yeri incelemesi" denir. Adli olaylarda, özellikle cinayet olaylarının bir bölümünde, olay yeri incelemesi sırasında mağdur ve suça ilişkin kanıtları olay yerinde gözlemlemek olasıyken bir kısım olaylarda ceset ve suça ilişkin kanıtlar yeraltına gömülerek yok edilmeye çalışılmış olabilir.



Pulse EKKO IV ve Basitleştirilmiş Yer Radarı çalışma prensibi

"Mezar yeri tanımlaması çalışmasına" alan taramasıyla ve yerden ve/veya havadan çekilen fotoğraflarla başlanır. Alan taraması tamamlandıktan sonra, yani özel olarak eğitilmiş köpeklerle yapılan olay yeri inceleme ekiplerinin çalışmaları, entomoloji (böceklerin yaşamı ve çevreleri ile olan ilişkilerini inceleyen bilim dalı) uzmanlarının incelemeleri, metan gazı analizi üzerine yapılan çalışmalar, botanik uzmanlarının çalışmaları ve bulguların tamamı değerlendirilerek kazı alanı belirleme çalışmaları yapılır. Bütün bu çalışmalar sonunda, kazılacak alandan emin olunamıyorsa ve cinayetle ilgili kanıtlar yok edilmeden yer belirleme işlemi gerçekleştirilmek isteniyorsa jeofizik yöntemlerle mezar yeri saptama konusu gündeme gelir.

1990 yılından beri, gömülü insan kalıntılarını araştırma çalışmaları büyük ölçüde jeofizik uygulamalarla gerçekleştiriliyor. Jeofizik, fiziğin ilkelerinin yerkürenin incelenmesine uygulanması demektir. Tıpta bilinen yöntemlerin birçoğu jeofizikte yeryüzüne uygulanır. Örneğin, bir doktorun hastasının hikâyesini dinlemesiyle jeofizikçilerin araştırma yapacakları konuyu irdelemeleri (örneğin MR (manyetik rezonans görüntüleme) benzeri bir uygulamayla yerin elektromanyetik yöntemle incelenmesi) ve bir doktorun hastasının sırtına ve karın boşluğuna parmakla vurarak çıkan sesi dinlemesiyle de jeofizikte sismik yöntem uygulamaları eşleştirilebilir. Adli jeofizik ise, adli araştırmalarla ilişkili jeofizik yöntem uygulamalarıyla yeraltında ya da su altında bulunan gömülü nesnelerin (ceset, mezar veya suçluyla ilişkili deliller) yerlerinin bulunması çalışmasıdır. Arama hedefi, genellikle cinayet araştırmalarında yaklaşık 0,5-1 m'ye gömülmüş cesetlerin, silahların ya da kayıp araçların bulunduğu yerlerdir.



Yer radarı çalışması ile (pamuklu bir örtüye sarılarak) 0,5 m derine gömülen domuz kalıntısının yerinin belirlenmesi

Adli Jeofizik Araştırmalarda Tercih Edilen Jeofizik Yöntemler

Jeofizik yöntemde yer radarı (*ground penetrating radar* - GPR) ile mezar yerini tanımlamada başarılı sonuçlar elde edilmektedir. Diğer yöntemler, yani elektrik özdirenç ve manyetik yöntem uygulamaları üzerine araştırmalar ise halen devam etmektedir.

Radar, radyo dalgalarını kullanarak mesafe ve ışık koşulları nedeni ile göremediğimiz cisimlerin bulundukları yeri ve konumu belirlemek için geliştirilmiş bir cihazdır. Yer radarıysa yeraltının araştırılmasında (en fazla 50-60 metre derinlikten bilgi alınabilmektedir) kullanılan bir aygıttır. Yer radarı uygulamasında, yer içine yüksek frekanslı elektromanyetik dalgalar (EM) gönderilir. İlerleyen dalgalar, optikte olduğu gibi ortam değiştiğinde ara yüzeylerde kırılma ve yansımaya uğrar. EM dalgalar farklı dielektrik özelliği olan bir yüzey yapısıyla karşılaştıkları zaman yansıyarak yeryüzüne geri döner. Yöntem, geri dönen dalgaların yeryüzündeki alıcıyla kaydedilmesi esasına dayanır. Günümüzde özellikle arkeolojik araştırmalarda çok yaygın kullanım alanı bulan yer radarı uygulamaları, ceset kalıntılarının aranmasına dönük çalışmalarda da oldukça başarılı sonuçlar verir.

Adli araştırmalarda yer radarı yöntemiyle başarılı sonuçlar elde edilse de, yöntemin uygulamasında bazı alanlarda (yüksek iletkenlik gösteren ortamlarda) gözlenen çözümsüzlük, başka yöntemlerin de kullanılmasını gerektirmiştir.

Bunlardan elektrik özdirenç yöntemi, yeryüzüne yerleştirilen iki elektrotla yeraltına verilen elektrik akımının oluşturacağı gerilim farkının, başka iki elektrot yardımıyla ölçülerek yeraltı yapısının incelenmesi ilkesine dayanır.

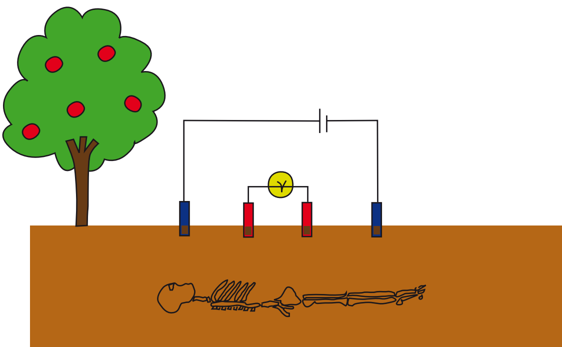
Yeraltı tekdüze ise, iki akım elektrodu arasındaki iletim sonucu, ortamın iletkenliğine bağlı olarak gerilim elektrodları arasında bir gerilim farkı ölçülür. Ortamda tekdüzeliği bozan herhangi bir olgu

varsa iletim etkileneceğinden, ölçülen gerilim farkı değerlerinde belirgin bir değişim gözlemlenir. Gerilim fark değerlerinden yararlanılarak, doğal ve yapay yeraltı yapılarının özdirenç değerlerine ulaşılabilir. Bir başka deyişle yeraltı elektrik özdirenç yöntemiyle, elektriği iletme ya da iletememe özelliğine göre haritalandırılır.

Manyetik yöntemdeyse, yerin manyetik alanındaki değişimler saptanmaya çalışılır. Yeraltında bulunan bir cismin manyetik belirti verebilmesi için, cismin manyetik duyarlılığının kendisini çevreleyen kayaçların manyetik duyarlılığından farklı olması gerekir. Manyetik alanın şiddetini ölçen cihazlara manyetometre denir.

Adli araştırmalarda manyetik yöntem uygulamaları son dönemin önemli araştırma konularından biridir. İnsan vücudunun manyetik duyarlılığı düşüktür ve çoğu kez ölçüm sonuçları ayırt edici bir belirti sunamaz. Bu nedenle bu yöntem, doğrudan ceset aramakta kullanılmaz, daha çok ortamı bozularak açılmış mezar yerlerinin sınırlarının saptanmasında bu yöntemden yararlanılır.

Başarılı bir sonuç elde etmek için, araştırma yapılan konuya ve çalışma alanına uygun yöntem seçimi çok önemlidir. Bir jeofizik çalışmada ölçümlerin sonuçlarını yorumlarken, yerel koşullar, gömülme zamanı, aranan hedefin boyutu ve aranan hedefin çevresini saran malzeme yapısı, yeraltı su seviyesiyle taşınma gibi koşulların da göz önüne alınması gerekir. Jeofizik çalışma, adli araştırmalarda yüksek başarı oranı sağlar. Gözlemsel yollarla yapılan çalışmalarda, örneklenen çalışma alanında tüm alanın ancak % 5'lik bir kısmı taranabilirken, jeofizik çalışmayla bu oran % 95'i bulur. Jeofizik çalışmaya ayrılması gereken süre daha uzundur ve işlem maliyeti de deneme çukuru açarak hedef yeri belirlemeye göre iki kat fazladır. Ancak, mezar yeri tespitinde deneme çukurlarıyla gömülmüş cesede ulaşma oranı % 10'un altında kalırken, jeofizik ölçümlerle bu oran % 90'ın üzerine çıkarılabilir.



Elektrik özdirenç yönteminin arazi uygulamasının şematik gösterimi.



Visual Photos

Günümüzde adli bilimler çalışma alanı, suçlu sayısının ve suçların artışına koşut olarak gelişen teknolojiyle kendine yeni çalışma alanları açıyor ve farklı bilim dallarının bir araya gelmesiyle kurulan enstitüler ve resmi kurumlar aracılığıyla gelişimini sürdürüyor. Yurt dışında iki yüzden fazla üniversitede adli bilimler eğitimi veriliyor ve bu konuda her yıl çok sayıda yayın yapılıyor. Ülkemizde Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara Üniversitesi Adli Tıp Enstitüsü ve İstanbul Üniversitesi Adli Tıp Enstitüsü yüksek lisans ve doktora eğitimi programlarıyla adli bilimler konusunda uzmanlar yetiştiriyor. Ankara Üniversitesi Tıp Fakültesi Adli Tıp Anabilim Dalı'nca yayımlanan Adli Bilimler Dergisi de bu konuda yapılan çalışmaların paylaşılmasına önemli katkılar sağlıyor.

Kaynaklar

Elbek, Ş., Ekinci, Y. L., Demirci, A. ve Koç, G., "Jeofizik Yöntemlerin Adli Araştırmalarda Kullanımı: Elektrik Özdirenç Tomografi Uygulaması", Poster Bildiri, GARS 2008.
Fenning, P. J. ve Donnely, L. J., "Geophysical Techniques for Forensic Investigation", *Geological Society*, Sayı 232, s. 11-20, 2004.
Murray, R . C. ve Tedrow, J. C. F., *Forensic Geology*, Prentice Hall, 1992.
Powell K., "Detecting Buried Human Remains Using Near-Surface Geophysical Instruments", *Exploration Geophysics*, Sayı 35, s. 88-92, 2004.
Ruffell, A. ve McKinley J., "Applications of Geology, Geomorphology and Geophysics to Criminal Investigations", *Forensic Geoscience: Earth Sciences Review*, Sayı 69, s. 235-247. 2005.

Figen Kadırgan

*Prof. Dr., Kimya Bölümü,
Fen-Edebiyat Fakültesi,
İstanbul Teknik Üniversitesi*

Yeni Bir Güneş Enerjisi Teknolojisi: Nano Kaplama

Günümüzde dünya nüfusundaki artış ve buna bağlı olarak enerji ihtiyacındaki artış, alternatif yakıtlara daha çok önem verilmesine ve buna bağlı olarak bu konuya daha fazla zaman ve para ayrılmasına neden oluyor. Var olan fosil yakıt kaynaklarının, enerji üretimi sırasında kükürt, azot oksitler gibi bazı zararlı kimyasallar üreterek çevreye verdiği zarar düşünüldüğünde, konuya verilen önemin artmasının normal olduğu düşünülebilir.


JUPITERIMAGES

Güneş enerjisinin öneminin yenilenebilir enerji eldesindeki payının giderek artması bekleniyor. Çünkü Güneş Dünya'ya tükettiğimiz toplam enerjiden 10.000 kat daha fazla enerji yollar ve çevre dostu bir enerji kaynağıdır. Gelişmiş ülkelerde endüstride (fabrikalarda ve organize sanayi bölgelerinde) ve yerleşim alanlarında (evlerde, sitelerde) termal (sıcak su, radyatör ön ısıtma, havuz ısıtma) yüksek verimle termal dönüşüm uygulamalarına çok sık rastlanıyor.

Elektrik Etüt İdaresi Genel Müdürlüğü (EİE) tarafından yapılan çalışmaya göre Türkiye'nin ortalama yıllık toplam güneşlenme süresi 2640 saat (günlük toplam 7,2 saat), ortalama toplam ışınım şiddetiyse 1311 kWh/m²-yıl (günlük toplam 3,6 kWh/m²) olarak belirlenmiştir. Ancak bu değerin, Türkiye'nin gerçek potansiyelinden daha az olduğu, daha sonra yapılan çalışmalar ile anlaşılmıştır. 1992 yılından bu yana Elektrik Etüt İdaresi Genel Müdürlüğü ve Devlet Meteoroloji İşleri Genel Müdürlüğü (DMİ), güneş enerjisi değerlerinin daha sağlıklı olarak ölçülmesi amacıyla enerji amaçlı güneş enerjisi ölçümleri alıyor. Devam eden ölçüm çalışmalarının sonucunda, Türkiye güneş enerjisi potansiyelinin eski değerlerden % 20-25 daha fazla çıkması bekleniyor.

İstanbul Teknik Üniversitesi Kimya Bölümü'nde yaptığımız çalışmalar, güneşle termal (ısıl) ısıtma, güneş pilleri ve hidrojen enerjisiyle bağıntılı yakıt hücreleriyle ilgili teknolojilerin geliştirilmesi üzerine yoğunlaşıyor. Bu yazıda yapmakta olduğumuz çalışmalardan güneş enerjisinin termal dönüşümü ile ilgili gelişmeler üzerinde duracağız.

Termal Dönüşüm

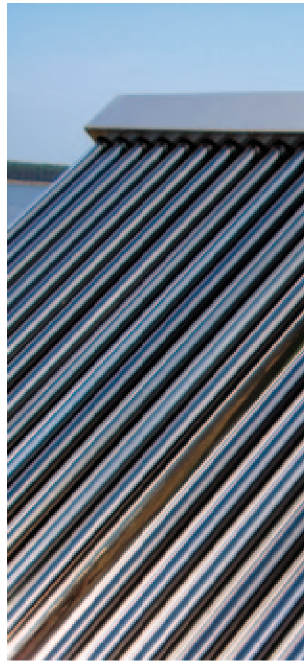
Binalardaki enerji harcamalarının kontrollü olmasının önemi göz ardı edilemez. Yapılan çalışmalar toplam enerji harcamalarının % 40'ının binalara ait olduğunu gösteriyor. Kyoto Protokolü'ne göre

2012 yılına kadar sera gazları salımının % 8 oranında düşürülmesi gerektiği için, binaların enerji harcamalarının önemi ortaya çıkıyor. AB ülkelerinde binaların enerji performansını ölçen ulusal kurallar ve canlandırma programları var. Ülkemizde de bu konuda çalışmalar sürüyor.

Güneş enerjisinin yüksek verimle termal dönüşümü konusunda yatırım alanlarını ve uygulamaya dönüşebilecek yenilikçi alanları şu başlıklar altında toplayabiliriz: Yüksek verimle termal enerji (ısı) eldesi (binaların, turistik tesislerin, ticari binaların enerji harcamalarının yaklaşık % 60'ının ısı enerjisi olduğu göz önüne alınırsa yüksek verimle enerji eldesinin önemi göz ardı edilemez), termal elektrik eldesi (güneş pilleri ile elde edilen elektrik enerjisinin 1000'lerce katı), güneş enerjisi ile soğutma yapma, yani soğurmalı soğutma sistemleri, deniz suyundan tatlı su eldesi, meyve-sebze kurutma.

Ülkemizde yüksek verimli termal dönüşüm teknolojisi kullanılmıyor. Yarı seçici yüzey üreten bir firma dışında, güneş kollektörlerinin yüzeyleri mat siyah boya ile boyanarak hazırlanıyor. Bunlarda da profil yüzeylerinin soğurma-yayma oranı çok düşük. Dolayısıyla güneşle ısınan su, ısısını ışınımla hızla kaybediyor. Siyah mat boya ile hazırlanan yüzeylerde boya çatlaması ve korozyona çok sık rastlanıyor ve bu yüzeylerin ömürleri de kısa oluyor.

Yüksek verimli kollektör yüzeyleri güneş ışığına karşı seçici ve koruyucu kaplamalardan oluşur. Yüksek verimli bir kaplamanın güneş ışığını, ısı verdiği dalga boyu aralığında olabildiğince fazla soğurması gerekirken, radyasyonla ısı kaybının olduğu dalga boyu aralığında da yüzeyin olabildiğince düşük ışıma yapması gerekir. Bu kaplamalar 1 μm'den (milimetrenin binde biri) daha ince filmlerdir (nano incelikte) ve vakum teknikleri ya da elektrokimyasal kaplama yöntemleri ile hazırlanırlar.


JUPITERIMAGES

İTÜ-KOSGEB ortaklığı ile güneş enerjisinin termal dönüşümü konusunda yapılan çalışmalar bakır, alüminyum ya da sac yüzeylerin güneş ışığına karşı seçici ince filmlerle kaplanmasını ve bu yüzeylerin yüksek verimli kollektörlerin üretiminde kullanılmasını amaçlıyor. Bu çalışmada güneş ışığını belirli dalga boyları aralığında yüksek değerlerle soğuran, buna karşılık yayma değeri düşük nano filmler, bakır veya sac yüzeyler üzerine elektrokimyasal kaplama yöntemi ile kontrollü bir şekilde kaplanıyor. Patent altında korunan bu yöntemle,, metal yüzeyler üzerinde kademeli olarak elektrokimyasal kaplamalarla nikel siyahı filmler oluşturuluyor. Oluşturulan filmlerin yüksek sıcaklığa ve korozyona dayanıklılığı test edilmiş durumda. Yöntem Avrupa'da vakum tekniğiyle üretilen sayılı benzerlerine oranla çok daha dayanıklı ve üretim tekniğinin basitliği nedeniyle de çok daha ucuz.

Yüksek verimli bu yüzeylerin spektral özellikleri aşağıdaki şekilde gösteriliyor: Görüldüğü gibi soğurma katsayısı 0,95'in üzerindeyken emisyon katsayısı 0,07.

Bu yüzeyin sürekli ve ucuz bir yöntem ile rulodan ruloya sarılarak üretimini pilot tesis altında geliştirmek için İTÜ-KOSGEB altında kurulan "Selektif Teknoloji" Ar-Ge şirketi faaliyete başlamak üzere.

Güneş enerjisi ve uygulamalarının ülkemizde yeni teknolojiler ile hızla yerini alması gerekiyor. Fotovoltaik teknoloji, ancak orta ve uzun vadede yatırıma dönüşebilir, çünkü ülkemizde araştırma geliştirme aşamaları henüz tamamlanmamış durumda. Türkiye'nin göz ardı etmemesi gereken konu termal dönüşümdür. Almanya 2002'den günümüze kollektör üretimini 3 kat arttırmıştır, bugün de Avrupa'da en fazla seçici yüzey üretimi yapan ülkedir. İspanya, Madrid Bildirgesi ile yeni yapılan binalarda güneş kollektörlerinin kullanımını zorunlu kıldı. Bu bir devlet teşviğidir.

Bu teknolojilerin binalara uygulanması ise estetik yönü düşünülerek ve enerji verimini azaltmayacak şekilde yapılmalı. Konutlarda güneş kollektörleri sadece çatılarda değil, estetik bir şekilde cephelere yerleştirilerek de kullanılabilir. Enerji uygulamalarında beş E'nin bir arada olması önemlidir: Enerji, Ekonomi, Ekoloji, Etik ve Estetik. Ama asıl başlangıç noktası altıncı E'den yani Eğitim'den geçiyor.

Bu teknolojinin geliştirilerek yatırıma dönüşmesi son derece önemli. Bunun için, teşvik yasalarında sadece güneş elektriğine değil, güneşten yüksek verimle elde edilecek ısıya da finansal desteklerin ne şekilde verileceğinin tartışılması gerekli.

Kaynaklar

Kadırgan, F., Sohmen, M., "Electrodeposited Black Cobalt Selective Solar Absorber Films and Their Characterization", *Renewable Energy*, Sayı 16, Cilt 4, s. 2304, 1998.
Suzer, S., Kadırgan, F., Sohmen, M., Wetherilt, J., Ture, E., "Spectroscopic Characterization of Al_2O_3-Ni Selective Absorbers for Solar Collectors", *Solar Energy and Materials*, s. 52-55, 1998.
Suzer, S., Kadırgan, F., Sohmen, M., "XPS Characterization of Co and Cr Pigmented Copper Solar Absorbers", *Solar Energy Materials and Solar Cells*, Sayı 56, s. 183, 1999.
Kadırgan, F., "Electrochemical Nano-Coating Processes in Solar Energy Systems", *International Journal of Photoenergy*, Sayı 84891, s. 1-5, 2006.
Kadırgan, F., Sohmen, M., Wetherilt, J., Ture, E., "Elektrokimyasal Olarak Spektral Seçici Yüzeylerin Geliştirilmesi", Türk Patent Enstitüsü, 1998.
Kadırgan, F., Method of depositing selectively absorbent film on a metal substrate Patent, PCT/TR2003/000081, WO 2005/042805

Dr. Bülent Gözcelioğlu

Denizlerimizdeki Yabancılar



Tersyüz denizanası (Kızıldeniz göçmeni)

Türkiye'nin farklı özellikleri olan dört denizi var. Güneyde sıcak ve çok tuzlu Akdeniz, kuzeyde soğuk ve az tuzlu yapıdaki Karadeniz ile bu iki deniz arasında bağlantıyı sağlayan ve her iki denizin özelliklerini taşıyan Marmara ve Ege denizleri. Denizlerimizdeki bu farklılıklar değişik özellikte çok sayıda türün sularımızda yaşamasına olanak sağlıyor. Diğer taraftan bu canlı çeşitliliğini tehdit eden kirlenme, kıyıdaki yapılaşmalar, endüstriyel gelişmeler, tarımsal faaliyetler gibi çok sayıda etken var. Bunlara bir de yabancı türler ve bunlardan kaynaklanan biyolojik istila eklendiğinde denizel biyoçeşitliliğimizin tehlike altında olduğu kolayca anlaşılabilir.

Denizler, yabancı türlerden ve biyolojik istiladan en fazla etkilenen sistemler. Bunun insan kaynaklı çok sayıda nedeni var. Deniz taşımacılığı, akvaryumculuk, kültür balıkçılığı ve diğer yetiştiricilik etkinlikleri gibi nedenler başta geliyor. Deniz taşımacılığı türlerin bir yerden bir yere taşınmasında, istemeden de olsa, kolaylık sağlıyor. Türlerin bu biçimde bir yerden başka bir yere taşınmalarının deniz ticaretiyle (antik çağlardan günümüze) başladığı söylenebilir. Deniz taşımacılığı aracılığıyla taşınma, gemilerin alt tarafında tutunma ya da balast sularıyla olabilir. Yapışıcı ya da delici özellikleri olan organizmalar (bazı deniz solucanları, bazı yumaşakçalar vb.) gemilerin alt tarafına tutunarak çok uzak mesafelere kolayca gidebilirler. Balast sularıyla taşınımdaysa çok sayıda tür bir yerden bir yere taşınabilir. Balast suları gemilerin dengelerini sağlamak için boş tanklarına aldıkları büyük miktarlardaki deniz suyudur. Bu suda plankton, omurgasız türleri, balık ve bazı türlerin larvaları gibi çok sayıda deniz canlısı bulunur. Balast suyu alımı, taşınması ya da boşaltımı sırasında canlılar genellikle yaşamlarını kaybederler. Özellikle boşaltım sırasında, çoğu kez (tuzluluk ve sıcaklık farkından dolayı) doğal ortamlarından çok farklı bir ortamla karşılaşırlar ve büyük bir çoğunluğu da bu sırada ölür. Ancak, farklı tuzluluk ve sıcaklık değerlerinde yaşayabilen bazı türler bu değişikliğe dayanabilir ve girdikleri yeni ortamda yaşamlarını devam ettirebilirler. Ekolojik toleransı yüksek canlılar olarak nitelenen bu türler, girdikleri yeni ortamda bazen çok büyük koloniler de oluşturabilirler.

Deniz akvaryumu yoluyla yabancı tür girişi genelde akvaryumun bilinçsizce denize boşaltılmasından kaynaklanır. Buna en iyi örnek, bilimsel adı *Caulerpa taxifolia* olan katil yosundur. Katil denmesinin nedeni bulundu-

bulent.gozcelioglu@tubitak.gov.tr

ğu ortamda hemen hemen her yeri kaplayarak diğer canlıların yaşam alanını işgal edip, onlara yaşama alanı bırakmaması. Katil yosunun doğal yayılış alanı Hint Okyanusu ve Karayip Denizi. Doğal ortamında herhangi bir tehlike yaratmayan bu tür, Akdeniz'de diğer canlıların yaşam alanlarını tehdit ediyor. Peki, bu duruma nasıl gelindi? Katil yosun, Avrupa'ya ilk olarak 1980'lerde Almanya'daki deniz akvaryumları için getirildi. Akvaryumda bakımı kolay olan, rengi solmayan ve güzel görüntü oluşturan bu yosun türü kısa sürede akvaryumcuların gözdesi oldu. Buradan Monaco'daki deniz akvaryumuna getirilen tür, yanlışlıkla havuzun boşaltım sistemiyle denize karıştı ve 1984'te ilk kez Akdeniz'de görüldü. Başlangıçta küçük bir alanda yayılış gösteren katil yosun altı yıl içinde başarılı bir uyum süreci geçirdi ve gittikçe hızlı biçimde yayılmaya başladı. Bugün Batı ve Orta Akdeniz'de birçok ülkede görülüyor. Bilim insanları, doğal ortamında istilacı özellik göstermeyen bu türün Akdeniz'de istilacı olmasının nedenini, Akdeniz'de doğal düşmanının olmamasına ve akvaryumda daha dayanıklı hale gelmesine bağlıyorlar. Katil yosun henüz ülkemiz kıyılarında yok. "Henüz" diyoruz çünkü kıyılarımıza gelme olasılığı oldukça yüksek. Batı Akdeniz'den kalkan herhangi bir geminin çapasında bile gelebilecek durumda.

Süveyş Kanalı

Doğal ekosistemlere insan kaynaklı yabancı tür girişinin bir nedeni de farklı ekosistemlerin kanallarla birbirine bağlanması. Buna en iyi örnek Süveyş Kanalı. 1869'da açılan bu kanal, Akdeniz ile tropik bir deniz özelliği gösteren Kızıldeniz ve Hint Okyanusu'nu birbirine bağladı. Ekosistemler arasında canlı geçişine de olanak sağlayan bu kanaldan türler 20-30 yıldan sonra yavaş yavaş geçmeye başladı. Daha çok Kızıldeniz'den Akdeniz'e geçiş yapan türlerin sayısında son yıllarda çok artış var. Bugün Akdeniz'de yapacağınız her dalışta Kızıldeniz kökenli türleri görebilirsiniz. Kızıldeniz kökenli türlerin girişi bu hızla devam ederse gelecekte yerli türleri görmek çok zor olacak; çünkü Kızıldeniz kökenli türler, yerli türler üzerinde kolayca baskı kurarak onların ortamdan uzaklaşmasına neden oluyor.

Yabancı Türlerimizden Örnekler

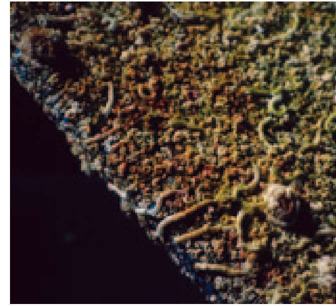
Ülkemiz denizlerinde yabancı tür sayısı 2005 yılında yapılan bir çalışmaya göre 263 olarak belirlenmiş. 2005'ten sonra bulunan yabancı türlerle birlikte bugün bu sayının 280'den fazla olduğu tahmin ediliyor. Yabancı türlerden bazıları zararlı ve yıkıcı etki gösterirken bazılarının ekosistemin dengesini bozacak herhangi bir etkisi yoktur. Örneğin, İzmir'de görülen *Alexandrium tamarense*, *Heterosigma akashiwo*, *Gymnodinium mikimotoi* gibi planktonlar toksik özelliktedirler ve? aşırı çoğaldıklarında ekosistem için zararlı etkiler yaratırlar. Karadeniz'de 1980'lerde ortaya çıkan *Mnemiopsis leidyi* adlı Atlantik kökenli bir taraklı hayvan türü hamsi popülasyonuna çok zarar vermiş ve bir dönem hamsi balıkçılığı durma noktasına gelmişti. Ancak 1990'ların sonunda, bununla beslenen *Beroe ovata* adlı başka bir yabancı tür Karadeniz'e gelmiş ve *Mnemiopsis leidyi*'nin artışı durmuştur. Bir başka örnek, *Rapana venosa* adlı deniz salyangozu. 1960'ta Karadeniz'de kaydı tutulan bu tür, karadeniz'deki midye popülasyonuna çok zarar vermişti. 1990'larda Marmara'da ortaya çıkan Atlantik kökenli *Asterias rubens* adlı denizyıldızı da midye popülasyonlarına zarar vermişti. Bununla birlikte Kızıldeniz kökenli türlerden bazılarının (sokar balığı gibi) avcılığı yapılarak ekonomik yarar da sağlanabiliyor. Her ne kadar bazıları zararsız ve hatta ekonomik değer taşıyor olsa da yabancı türlerin doğal ekositemler için her zaman bir tehdit olduğu unutulmamalı.



Külah balığı (Kızıldeniz göçmeni)



Sokar balığı (Kızıldeniz göçmeni)



Yapışıcı ya da delici özellikleri olan organizmalar (bazı deniz solucanları, bazı yumaşakçalar vb.) gemilerin alt tarafına tutunarak çok uzak mesafelere kolayca gidebilirler.

Fotoğraflar: Dr. Bülent Gözcelioğlu

Kaynaklar

Çınar, M. E., Bilecenoglu, M., Öztürk, B., Katagan, T., ve Aysel, V., "Alien Species on the Coasts of Turkey," *Mediterranean Marine Science*, Cilt 6, Sayı 2, 119-146, 2005.

Zenetos, A., Meriç, E., Verlaque, M., Galli, P., Boudouresque, C. F., Giangrande, A., Çınar, M. ve Bilecenoglu, M. , "Additions to the Annotated List of Marine Alien Biota in the Mediterranean with Special Emphasis on Foraminifera and Parasites," *Mediterranean Marine Science*, Cilt 9, Sayı 1, 119-165, 2008.

Cirik, Ş. ve Akçalı, B., "Denizel Ortama Yabancı Türlerin Taşınıp Yerleşmesi: Biyolojik Yapının Kontrolü, Hukuksal, Ekolojik ve Ekonomik Yönleri," *E.Ü. Su Ürünleri Dergisi*, Cilt 19, Sayı 3-4, 507- 527, 2002.,

http://www.ciesm.org/online/atlas/intro.htm

Doç. Dr. Ferda Şenel

Kenelerle Taşınan Hastalıklar


JUPITERIMAGES

Kene (Ixodoidea), eklem bacaklıların örümceğimsiler (Arachnida) sınıfından kan emici ve gözsüz bir dış parazit olarak tanımlanır. En sık olarak göçmen kuşlarla hastalıkları yaydığı bilinmektedir. İnsan, koyun, köpek, kedi, deve gibi canlıların derilerine yapışarak kanlarını emer. Uçamayan ve sıçrayamayan bu küçük hayvanlar yumurtlayarak çoğalır. Keneler, konakladıkları hayvanlarda bulunan çeşitli mikropları yutarak diğer hayvanlara veya insanlara taşır.

Keneler otlaklarda, çalılıklarda ve kırsal alanlarda yaşar. Oval şeklindeki erişkin kenelerin sekiz bacağı olur. İlk iki bacak çifti öne, son iki çifti geriye yönelmiştir. Bacakların uçlarında çengeller ve vantuzlar vardır. Deriye rahatça yapışarak hortumlarıyla kan emerler ve 12 milimetreye kadar şişebilirler. Yapıştığı hayvan veya insanın kanını emen kene, iyice şiştikten sonra kendini yere atarak konağından uzaklaşır ve otlara veya ağaçlara tırmanır. Daha sonra, kırsal alanda gezinen hayvan ve insanların üzerine düşerek tekrar onlara yapışır. Bugün 900'e yakın kene türü bilinmektedir. Türü ve boyutu ne olursa olsun tüm keneler kanıyla beslenebilecekleri konakların arayışı içindedir. Hayvan ve insanların kanlarını emerek beslenen keneler bu yolla onlara çeşitli hastalıklar bulaştırır. Küçük kemirgenler, yabani hayvanlar, evcil memeli hayvanlar ve kuşlar keneleri barındıran hayvanlar arasında sayılır. Bu hayvanlar, kenelerin ve taşıdıkları hastalık etkenlerinin varlığının sürmesinde önemli rol oynar.

Kırım-Kongo Kanamalı Ateşi (KKKA) Hastalığı

Kırım-Kongo kanamalı ateşi (KKKA) hastalığının ülkemizde de görülmesiyle son yıllarda halk ister istemez kenelerle daha fazla ilgilenir hale gelmiştir. Oldukça küçük sayılabilecek bu hayvanlar, KKKA hastalığının yanı sıra daha birçok ciddi hastalığa neden olabilir. KKKA hastalığına kenelerin taşıdığı nairovirüsler yol açar. *Hyalomma* türünden kenelerin, özellikle de *H. Marginatum marginatum*'un hastalığın taşınmasında oldukça etkili olduğu bilinmektedir.

Bir bölgede, keneleri taşıyan tavşan ve yaban domuzlarının çoğalması, o bölgede hastalığın artmasına yol açabilir. Hastalığı uzak ülkelere taşıyabilen göçmen kuşlar da KKKA hastalığının yayılmasında önemli rol oynar. Virüsle temas eden veya taşıyan hayvanlarda hastalık görülmez. Bu virüs sadece insanlarda hastalığa yol açar. Bağışıklık sistemi ve damar hücrelerine saldıran virüsler, kendilerine karşı antikor salgılanmasını engeller ve damar hücrelerinde hasara yol açar.

Virüsle temas eden her beş kişiden birinde hastalık görülür. Hastalığın kuluçka dönemi 3-7 gün arasındadır. Aniden çok yükselen ateş (41 °C'ye kadar), baş ağrısı, kas ağrıları, baş dönmesi hastalığın ilk belirtileri arasındadır. Bu belirtilere ek olarak ishal, bulantı ve kusma da görülebilir. Yüz, boyun ve göğüste kızarıklık, göz iltihapları da diğer belirtiler arasında sayılır. Hastalığın başlangıcından yaklaşık bir hafta sonra kanamalı dönem başlar. Kanama en sık olarak sindirim sistemi, cinsel organlar, idrar yolları ve solunum yollarında olur. Bu dönemde, dışkıda, idrarda veya balgamda kan görülmesi sık karşılaşılan bulgular arasındadır. Erken teşhis ve tedavi, hastalığın yayılımının önlenmesinde büyük önem taşır. Kene ısıran veya hastalığın sık görüldüğü kırsal bölgelerden gelen kişilerde ateş ve kas ağrıları varsa KKKA hastalığından şüphelenmek gerekir.

Etki mekanizması tam olarak bilinmese de günümüzde "ribavirin", KKKA hastalığında kullanılabilecek tek antiviral ilaçtır. Yeni ilaç adaylarından ribamidin ise ribavirinden 4,5-8 kat daha az etkilidir. Son yıllarda, vücutta interferon üretimini arttıran ve "MxA" olarak tanımlanan bir ilaç üzerinde çalışmalar yapılıyor. Bu ilacın virüste RNA sentezini engellediği belirtiliyor. Hastalığın yayılmasının önlenmesi ve erken teşhis Kırım-Kongo kanamalı ateşi ile mücadelenin temel unsurlarını oluşturuyor.

Anaplazmozis

Kenelerin bulaştırdığı hastalıklardan birisi de anaplazmozistir. Bu hastalık, *Anaplasma phagocytophilum* adlı bakterinin keneler tarafından taşınmasıyla oluşur. Geyik ve bazı fare türleri, anaplazmozis hastalığına yol açan bakterileri doğal olarak vücutlarında barındırır. Bu hayvanlar üzerinde bulunan keneler de bakteriyi insanlara taşır. Bu kene türlerinin Karadeniz bölgesinde de tespit edilmesinden sonra, anaplazmozis hastalığı ülkemizde dikkat çekmiştir. Anaplazmozis, bağışıklık sistemi zayıflamış kişilerde, kanser hastalarında ve HIV virüsü taşıyanlarda ölüm riski oluşturur. Anaplazmozise bağlı şikâyetler kene ısırmasından bir hafta sonra başlar. Ateş, şiddetli baş ağrısı, halsizlik ve kas ağrıları en sık görülen şikâyetler arasındadır. Hastalığın teşhisi, kanda yapılan bazı mikrobiyolojik incelemeler veya PCR tekniğiyle konulur. Tedavisinde tetrasiklin grubu antibiyotikler kullanılır.

Babesiozis

Babesiozis, kenelerle taşınan ve kırmızı kan hücrelerini etkileyen bir hastalıktır. Hastalığa yol açan *Babesia microti* adlı parazit, beyaz ayaklı farelerde ve küçük memelilerde yaşar. Parazit, kenelerle insanlara taşınır. Gelişim evresindeki keneler kan emmek için insan derisine tutunduğunda parazit vücuda girer. Babesia genellikle hiçbir şikâyete yol açmaz. Bazı kişilerdeyse, ateş, baş ağrısı, kas ağrıları, halsizlik ve iştahsızlık gibi, grip benzeri şikâyetler

mfsenel@yahoo.com.tr

görülebilir. Babesia parazitleri kırmızı kan hücrelerine saldırdığı için kansızlığa yol açabilir. Dalağı alınmış kişilerde, bağışıklık sistemi zayıflamış hastalarda, böbrek veya karaciğer yetmezliği olanlarda ölümcül seyredebilir. Tedavide, ateş düşürücü ilaçlarla birlikte bazı antibiyotikler 7-10 gün kullanılır.

Lyme Hastalığı

Hastalığa esas olarak "spiroket" denilen bakteriler yol açar. Bu bakteriler geyiklerin midesinde bulunur. Kene geyiği ısırdığında mikrop keneye geçer. Bakteriyi alan kene daha sonra bir insanı ısırdığında hastalık kişiye bulaşır. Dünyada kene ile taşınan en yaygın hastalık olan Lyme hastalığı, insandan insana geçmez. Hastalık, cildi, eklemleri, kalbi ve sinir sistemini etkiler. Hastalığın ilk belirtileri kenenin ısırdığı yerde oluşan yaralar ve kaşıntıdır. Daha sonra grip benzeri şikâyetler görülür. Isırığın olduğu bölgedeki lenf bezecikleri şişer, ciltte yaygın kızarıklık olur. Cilt yaralarından haftalar veya aylar sonra diğer organlar da etkilenmeye başlar. Eklemlerin etkilenmesine bağlı olarak, eklem ağrıları, eklem şişmesi ve hareket kısıtlılığı olur. Bakteriler kalp kasının iltihaplanmasına yol açabilir. Bu da kalp ritmini bozulmasına ve kalp yetmezliğine sebep olur. Sinir sistemini etkilemesi durumunda çeşitli bölgelerde duyu kaybı ve yüz felci görülebilir. Daha da kötüsü, bakteriler beyin zarı iltihabına (menenjit) da yol açabilir.

Lyme hastalığına karşı geliştirilen aşı, 1998 yılında Amerikan Gıda ve İlaç Dairesi (FDA) tarafından onay aldı. Yapılan çalışmalar bu aşının % 76-92 oranında bir koruma sağladığını gösterdi.

Tularemi Hastalığı

Tularemi, *Francisella tularensis* adlı bir bakterinin yol açtığı hastalıktır. Hastalık, mikrobu taşıyan kenelerin ısırmasıyla insanlara geçer. Kısa bir kuluçka süresinden sonra (3-5 gün) ateş, titreme, baş ağrısı, halsizlik, iştahsızlık, öksürük, karın ağrısı, ishal, kas ve göğüs ağrısı başlar. Kenenin ısırdığı ve mikrobun vücuda girdiği yerde derin yaralar oluşur. Bu bölgedeki lenf bezecikleri şişer. Eğer mikrop akciğerlere ilerlerse hayati sorunlara yol açabilir. Göğüs ağrısı, öksürük ve nefes darlığı görülür. Hastalığın en ciddi şekli olan akciğer tularemisi, tedavi edilmezse ölümle neticelenebilir. Çeşitli antibiyotiklerin 10-21 gün verilmesiyle hastaların tamamına yakını sağlığına kavuşur.

Erlikioz

Erlikioz hastalığına, *Ehrlichia* ailesinden bakteriler yol açar. İnsanlara kene ısırmasıyla bulaşır. Hastalık ilk kez 1935 yılında bir grup araştırma köpeğinde, 1986 yılında da insanlarda tespit edildi. Dünya genelinde yaygın bir hastalık olmasına rağmen vakaların çoğu ABD'de bildirilmektedir. Hastalık kene ısırmasından 5-10 gün sonra görülen baş ağrısı, kas ağrısı ve halsizlikle başlar. Bulantı, kusma, ishal, eklem ağrıları ve döküntü diğer şikâyetler arasındadır. Ancak hastalık bazı kişilerde çok hafif seyredebilir veya hiçbir belirtiye yol açmayabilir. Tetrasiklin grubu bir antibiyotikle kolayca tedavisi yapılır. Erlikioz hastalığı, tedavi edilmediğinde ölüme yol açacak kadar ağır seyredebilir.

Rocky Dağları Benekli Ateşi

Bu hastalığı "Amerikan köpek kenesi" olarak adlandırılan bir kene türü taşır. Hastalık çoğunlukla vahşi hayvan ve kenelerin birlikte bulundukları alanlarda ortaya çıkar. Hastalığa "riketsia" denilen bir mikrop yol açar ve insandan insana bulaşmaz . Riketsia, kan damarlarının duvarındaki hücreleri etkileyen bir hastalıktır. Hastalık sıklıkla 5-9 yaş arasındaki çocukları veya 60 yaş üzerindeki yaşlıları etkiler. Kene ısırmasından 5-10 gün sonra ateş, bulantı, kusma, iştahsızlık, baş ve kas ağrıları başlar. Ateşten 2-5 gün sonra önkol, el ve ayak bileği üzerinde küçük, düz, pembe ve kaşıntısız noktalar şeklinde benekli bir döküntü başlar. Hastalık, tedavi edilmezse beyin ve akciğerleri etkileyerek % 25 oranında ölüme yol açabilir. Bu nedenle en kısa sürede antibiyotik tedavisine başlanması gerekir. Hastalık erken teşhis edilir ve tedaviye başlanırsa hızlı bir düzelme gösterir.

Kolorado Kene Ateşi

Kolorado kene ateşi hastalığına bir ağaç kenesiyle bulaşan orbivirüsler yol açar. Çoğunlukla ABD'nin Rocky Dağları bölgesinde görülen bu hastalık, genellikle bağışıklık sistemi zayıf olan ve dalağı alınmış kişileri etkiler. Kene ısırmasından bir hafta sonra grip benzeri şikâyetler başlar. Yüksek ateş, döküntü, gözlerde kızarma en önemli belirtiler arasındadır. Hastalık, beyin zarı iltihabına (menenjit) dahi yol açabilir. Özel bir tedavisi olmayan Kolorado kene ateşi hastalığı genellikle 7-10 gün kadar sürer.

Kenelerden Korunmak

- ***İnsanlara hastalık geçmesi, kenelerden uzak durularak önlenebilir. Bu nedenle de mümkün olduğu kadar kenelerin bulunduğu alanlara gitmemek gerekir. Kenelerin yoğun olabileceği çalılık ve gür ot bulunan yerlerden uzak durulmalı, buralara çıplak ayakla ya da kısa giysilerle gidilmemelidir.***
- ***Kırsal alanlara av ya da görev gereği gidenlerin lastik çizme giymeleri, pantolonlarının paçalarını çoraplarının içine sokmaları gerekir. Bu sayede kenelerin pantolon paçalarından içeri girmesi önlenir.***
- ***Kırsal alanlara gidildiğinde, üzerindeki kenelerin kolayca görülebilmesi için açık renkli giysilerin tercih edilmesi önerilir.***
- ***Görevi nedeni ile risk altında olan kişilerin (sağlık personeli, veteriner hekim gibi), hasta hayvan ve insanların kan ve vücut sıvılarından korunmak için mutlaka eldiven, önlük, gözlük, maske kullanmaları gerekir.***
- ***İnsanları ve hayvanları kenelerden korumak için haşere kovucu ilaçlar kullanılmalıdır. Bu özel ilaçlar cilde sürülür veya elbiselere emdirilir.***
- ***Kenelerin bulunduğu alanlara gidildiği zaman vücut, muhtemel kene ısırığı açısından belli aralıklarla kontrol edilmelidir. Özellikle, koltuk altı, kulak içi ve çevresi, göbek deliğinin içi, dizlerin arkası, saç ve kıllı bölgelerin içi ve çevresi, bacak arası ve bel çevresi.***
- ***Vücuda yapışmış keneler uygun bir şekilde, ezilmeden, ağzından veya başından tutularak bir cımbız veya pens yardımıyla sağa sola oynatılarak alınmalıdır. Isırılan yer su, sabun veya alkolle temizlenmelidir. Mümkünse kenenin tanı için alkolde saklanması uygun olur.***
- ***Kırsal alanlara gittikten bir süre sonra ciltte kızarıklık oluşursa veya grip benzeri şikâyetler başlarsa hekime müracaat etmek gerekir.***

Kaynaklar

Barbour, A. G., Maupin, G. O., Teltow, G. J., Carter, C. J., Piesman, J., "Identification of an Uncultivable Borrelia Species in the Hard Tick Amblyomma americanum: Possible Agent of a Lyme Disease-like Illness", *Journal of Infectious Diseases*, Cilt 173, Sayı 2, s. 403-409, 1996.

Campbell, G. L., Paul, W. S., Schriefer, M. E., Craven, R.B., Robbins, K.E., Dennis DT., "Epidemiologic and Diagnostic Studies of Patients with Suspected Early Lyme Disease, Missouri, 1990-1993", *Journal of Infectious Diseases*, Cilt 172, Sayı 2, s. 470-480, 1995.

Rajput, Z. I., Hu, S., Chen, W., Arijo, A. G., Xiao, C. "Importance of Ticks and Their Chemical and Immunological Control Livestock, *Journal of Zhejiang University*, Cilt 7, Sayı 11, s. 912-921, 2006.

Ergönül, Ö., "Crimean-Congo Haemorrhagic Fever", *The Lancet Infectious Diseases*, Cilt 6, Sayı 4, s. 203-214, 2006.

Spach, D. H., Liles, W. C., Campbell, G. L., Quick, R. E., Anderson, D. E. Jr, Fritsche, T. R., "Tick-borne Diseases in the United States", *The New England Journal of Medicine*, Cilt 329, Sayı 4, s. 936-47, 1993.

Belman, A. L., "Tick-borne Diseases", *Seminars in Pediatric Neurology*, Cilt 6, Sayı 4, s. 249-266, 1999.

Nuhoğlu, İ., Aydın, M., Türedi, S., Gündüz, A., Topbaş, M., "Kene ile Bulaşan Hastalıklar" *TSK Koruyucu Hekimlik Bülteni*, Cilt 7, Sayı 5, 2008.

Teleskop Ayak ve Kurguları

Teleskopları tanıtmaya Mayıs sayımızda başlamıştık. Onların temel özelliklerine, nasıl çalıştıklarına değindikten sonra, geçen sayımızda da optik yapılarına göre tiplerine yer vermiştik. Çoğu kullanıcı, pek de bilinçli olmayan satıcıların da yönlendirmesiyle teleskopların yalnızca tiplerine ve optik özelliklerine göre teleskoplarını seçer. Bunlar, teleskopların en önemli özellikleri elbette. Ne var ki optik kalitesi ne kadar iyi olursa olsun, teleskop en hafif rüzgarda bile titriyorsa o teleskoptan istenen performansı elde etmek mümkün olmaz. Yine bu ay ele alacağımız "teleskop kurguları" (ayakla teleskop tüpü arasında bulunan ve teleskobun belli eksenlerde hareket etmesini sağlayan sistem) teleskop tipleri kadar önemli.

Teleskop Ayakları

Yukarıda da sözünü ettiğimiz gibi, mükemmel bir optik kalitesi olan bir teleskop en küçük hava akımında bile titriyorsa, bakılan cisim net olarak görülemez. Günümüzde kırtasiyelerde ve oyuncakçılarda satılan ucuz teleskopları saymazsak, çoğu teleskobun optik kalitesi kabul edilebilir düzeydedir. Ne var ki, özellikle ucuz modellerin önemli bir bölümü sağlam birer ayağa sahip değildir.



Bir teleskop satın almadan önce, teleskobun yere ne kadar sağlam "bastığı" sınanabilir. Bunun için teleskobun tüpüne hafifçe vurarak ne kadar süreyle sallandığını gözlemek yeterli. Eğer teleskop iki-üç saniyeden uzun süre boyunca gözle görünür bir biçimde titriyorsa, sağlam bir ayak üzerinde durduğu söylenemez. Bu kısa bir süre gibi görünebilir; ancak gözmerceğinden bakıldığında, görüntünün çok daha uzun bir süre titrediği görülür. Teleskop, bu ilk titreşim sınavını geçerse, göz merceğinden uzaktaki bir cisme bakarken, teleskobun ince ayar kollarını sırayla değişik yönlere çevirilmesiyle ikinci sınav uygulanabilir. Teleskoptaki görüntü yavaş ve sarsıntısız bir biçimde kaymalı. Bu sırada hafif bir titreşim olabilir. Ancak, ayar kolları bırakıldıktan hemen sonra, bu titreşimin durması gerekir. Elbette bu titreşim yalnızca teleskobun üzerinde durduğu üçayağa değil, kurgunun da sağlam olup olmadığına bağlıdır.

Kalın gövdeli ve ağır ayaklar genellikle daha sağlam ve titreşime karşı daha dirençli olurlar.

Teleskop Kurguları

Teleskop genel olarak düşünüldüğünde iki tür kurguya sahiptir. Bunlar, ufuksal (altazimuth) ve ekvatoryel kurgulardır. Ufuksal kurgu, fotoğrafçıların kullandığı üçayakların hareketini yapar. Yani bir eksende sağa ve sola, diğer eksende de aşağı ve yukarı hareket eder. Ufuksal kurgu daha çok yeryüzü gözlemleri için uygundur. Ancak, bazı ucuz teleskoplar ve ileride değineceğimiz üst model teleskoplar bu tür kurguya sahiptir.

Ekvatoryel kurgulu teleskoplarsa gökyüzü koordinatlarına göre (sağ açıklık ve dik açıklık) hareket edecek biçimde tasarlanmıştır. Bunun en büyük yararı yalnızca bir eksende ayarlama yapılarak, gökcismini izleme kolaylığı sağlamasıdır. Dünya'nın dönüşüne bağlı olarak gökyüzü, dev bir saat gibi 24 saatte bir çevremizde dönüyor görünür.

Teleskoplar, gökyüzünde çok dar bir alanı gösterdiklerinden, gözmerceğinden bakıldığında, bu hareket çok belirgindir. Bir gökcismi, birkaç saniye içinde görüntüden çıkar. İşte bu nedenle gözlemci gözlemini yaparken bir eliyle sağ açıklığı değiştirerek, Dünya'nın dönüşünü tersine izleyebilir. Ekvatoryel teleskopların çoğuna "izleme mekanizması" denen bir motor ve dişlilerden oluşan düzenek konularak bu izleme otomatik olarak yapılabilir. Birçok orta düzey teleskopta bu izleme mekanizmasının yanında, diğer



Ufuksal kurgulu elektronik kumandalı teleskop



Ekvatoryel kurgulu elektronik kumandalı teleskop



Dobson kurgulu teleskop

gokyuzu@tubitak.gov.tr

2009 Dünya Astronomi Yılı (DAY2009) Etkinlikleri - www.astronomi2009.org

TÜBİTAK 12. Ulusal Gökyüzü Gözlem Şenliği

24-27 ve 28-29 Temmuz 2009 - Antalya

Şenlik kapsamında 24-27 Temmuz 2009 tarihlerinde Saklıkent'te düzenlenecek olan "Uygulamalı Astronomi Etkinliği"nde temel bilgilerin verileceği görsel ağırlıklı seminerler, gökyüzünü tanıtmaya yönelik çıplak gözle yapılacak gözlemler, çeşitli gökcisimlerinin teleskoplarla gözlemleri, Saklıkent'in yakınında bulunan TÜBİTAK Ulusal Gözlemevi'ne (TUG) tanıtım gezisi ile çeşitli yarışma ve eğlenceli etkinlikler düzenlenecek.

28-29 Temmuz 2009 tarihlerinde düzenlenecek "Halka Açık Gözlem Etkinlikleri" sırasında TÜBİTAK Ulusal Gözlemevi Bilim ve Toplum Merkezi'nde (BİTOM) mevcut kurulu teleskobun yanındaki açık alanda kurulacak olan orta boy amatör teleskoplar ile uzmanlar eşliğinde gökcisimleri gözlenecek ve katılımcılara çeşitli bilgiler verilecek. Bu etkinliklere katılım serbest olacak.

24-27 Temmuz 2009 tarihlerinde düzenlenecek "Uygulamalı Astronomi Etkinliği"ne katılabilmek için başvurular yalnızca aşağıda bağlantısı verilen internet sitesindeki bilgiler doğrultusunda ve yine bu sitede yer alan başvuru formlarıyla yapılabilecek.

http://senlik.tug.tubitak.gov.tr/

13. Amatör Astronomi Yaz Okulu

29 Haziran - 01 Ağustos 2009 - İzmir

13. Amatör Astronomi Yaz Okulu, Ege Üniversitesi Gözlemevi'nde 29 Haziran - 01 Ağustos 2009 tarihleri arasında birer haftalık 5 dönem halinde yapılacak. Yaz okuluna, yaş sınırı olmaksızın gökbilime ve gökyüzüne meraklı herkes başvurabilir. Ancak kontenjan her dönem için 14 kişiyle sınırlı.

Yaz okulunda katılımcılara geceleri teleskoplarla gökyüzü gözlemleri yaptırılacak; ayrıca katılımcılar bilimsel gözlemleri izleme ve bu gözlemlerle ilgili bilgi alma şansı bulacaklar. Gündüzleriyse gökbilimle ilgili bilgiler verilecek. Katılımcılar dönem sonunda birer sertifika alacaklar. Bilgi ve başvuru için:
Prof. Dr. Serdar Evren
e-posta: serdar.evren@ege.edu.tr
Tel: (232) 373 14 03 - (232) 388 40 00 / 2322
http://astronomi.ege.edu.tr/yazokulu

İstanbul Kültür Üniversitesi DAY2009 Etkinlikleri

(http://fen-edebiyat2.iku.edu.tr/aas2009/)

2. Amatör Teleskop Yapımı Çalıştayı

4-9 Temmuz 2009 - İstanbul

İstanbul Kültür Üniversitesi'nin düzenlediği çalıştayda her biri 25 kişilik 4 gruba ayrılmış toplam 100 katılımcı birer 15 cm ayna çaplı teleskop yapacaklar. Atölyenin önemli bölümü teleskop aynalarının yapımına ayrılacak.

3. Amatör Astronomi Sempozyumu

10 Temmuz 2009 - İstanbul

Amatör gökbilimciler bu sempozyumda gözlemsel ve kuramsal çalışmalarını ve etkinliklerini paylaşacaklar.

Starfest09

10-11 Temmuz 2009 - İstanbul

10-11 Temmuz 2009 tarihlerinde düzenlenecek STARFEST09'da, Amatör Teleskop Yapımı Çalıştayı'nda yapılacak teleskoplarla beraber deniz kenarında müziğin ve astronominin ortak noktasında binlerce insan yıldızların altında buluşacak.

---

eksende de bir motor bulunur ve teleskop bir elektronik kumanda yardımıyla iki eksende de hareket ettirilebilir.

Günümüzde, bilgisayar kontrollü teleskopların sayısı giderek artıyor. Bu teleskoplar, istenen koordinata ya da bilgisayarın belleğine kayıtlı on binlerce gökcisminden seçtiğiniz birine kendiliğinden yönelebiliyor.

Günümüzde, büyük teleskop üreticileri bazı en üst modellerini ekvatoryel değil, ufuksal kurgulu olarak tasarlıyorlar. Aslında ufuksal kurguya sahip teleskopların izleme sistemleri karmaşık olur ve bilgisayar kontrolü gerektirir. Çünkü iki ekseni birden hareket ettirmek tek ekseni hareket ettirmekten daha karmaşıktır. Ancak, elektronik ve bilgisayar kontrollü sistemlerin ucuzlaması sayesinde artık birçok teleskop modeli bu sistemlerle birlikte piyasaya sürülüyor.

Bilgisayarlı teleskoplar genellikle elektronik olarak yönlendirildikleri için mekanik olarak daha karmaşık olan ekvatoryal kurgulara bazı özel durumlar dışında genellikle gerek duyulmaz. Ekvatoryal kurgulu otomatik teleskoplar genellikle gökyüzü fotoğrafçıları tarafından kullanılır. Çünkü kutup eksenine göre doğru bir şekilde ayarlanmış bir ekvatoryal teleskop bir gökcismini izlerken çok daha az hata yapar.

Günümüzde, teleskoplar o kadar otomatik hale geldi ki, gözlemciye gözmerceğinden gözlenmek istenen cisme bakmak dışında nereneyse hiçbir iş bırakmıyorlar. Öyle ki, bu teleskopların GPS'li (Küresel Konumlandırma Sistemi) olanları yeryüzündeki konumunu bile otomatik olarak saptayabiliyor. Gözlemciye, teleskobun veritabanında kayıtlı olan on binlerce gökcisminden birini seçip (gözlemci isterse bilgisayar kendisi de seçebilir) gözmerceğinden bakmak kalıyor. Ne teleskop kullanma becerisi, ne gökyüzünü çok iyi tanımak ne de gökyüzü haritası okuma becerisi gerekiyor.

Amatör gökbilimciliğin en zevkli yanlarından biri, gözlemek istediğiniz bir gökcismini kendi çabanızla bulabilmek kuşkusuz. Bu sadece teleskobu kullanmayı bilmekle değil, gökyüzünü iyi tanımayı, gökyüzü haritalarını kullanmayı bilmeyi de gerektiriyor. Bunlar, gözlem yaptıkça kazanılan deneyimler.

Deneyiminizi ve bilginizi kullanarak ve emek harcayıp, gözlemek istediğiniz bir gökcismini teleskobun görüş alanında gördüğünüzde mi daha çok zevk alırsınız, yoksa kumandaya yalnızca adını girdiğinizde size yalnızca gözmerceğine bakmak kaldığında mı? Deneyimli bir amatör gökbilimciyle deneyimsiz bir amatör gökbilimcinin bu soruya yaklaşımı farklı olacaktır. Deneyimli bir gökbilimci, bilgisayar donanımına harcayacağı paradan vazgeçerek, onun yerine daha büyük çaplı bir teleskop almak isteyebilir. Gökyüzünün derinliklerine dalmak isteyen deneyimsiz bir gözlemciyse, onu fazla zahmete sokmadan istediği gökcismine götürebilecek otomatik bir teleskobu tercih edebilir.

Son olarak, Dobson kurgusundan söz edeceğiz. Basit, kullanımı kolay ve ucuz bir teleskop kurgusu olan Dobson kurgusu, büyük çaplı teleskoba sahip olmak isteyen amatör gökbilimciler arasında çok yaygın. 1970'li yıllarda, John Dobson adlı bir amatör gökbilimcinin tasarladığı ve birkaç parça kontrplaktan yapılabilen bu kurgu, bir tür ufuksal kurgu. Dobson kurgusu, yalnızca basit ve ucuz bir kurgu olmasının yanı sıra, büyük çaplı Newton tipi teleskoplar için oldukça kullanışlı. Bilgisayarsız bir Dobson tipi teleskobu bir cisme yöneltmek ve bu gökcismini izlemek oldukça zordur. Bu tür kurgular genellikle motorsuz olsa da en gelişmiş teleskoplardaki sistemler bunlarda da kullanılabiliyor.

Alp Akoğlu

11 Temmuz
Jüpiter ve Ay yakın görünümde

13 Temmuz
Jüpiter Neptün'ün 0,6° güneyinde

14 Temmuz
Venüs Aldebaran'ın 3° kuzeyinde (sabah)

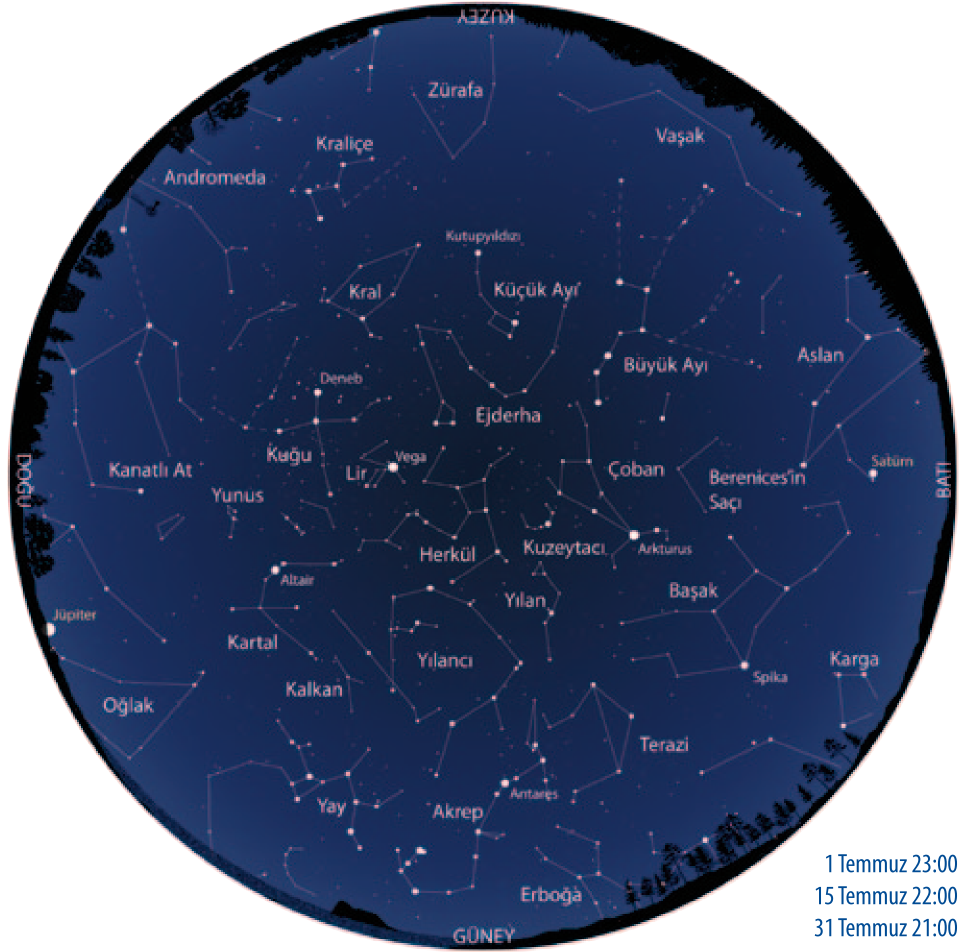
18 Temmuz
Mars ve Ay yakın görünümde; Ay, Ülker'in önünde (sabah)

19 Temmuz
Venüs ve Ay yakın görünümde (sabah)

22 Temmuz
Tam Güneş tutulması (Türkiye'den gözlenemeyecek)

25 Temmuz
Satürn ve Ay yakın görünümde (akşam)

31 Temmuz
Antares ve Ay çok yakın görünümde (akşam)



1 Temmuz 23:00
15 Temmuz 22:00
31 Temmuz 21:00

Temmuz'da Gezegenler ve Ay

Bu ayın en önemli gök olayı olan 22 Temmuz'daki tam Güneş tutulmasını ülkemizden izleyemeyeceğiz. Bu tutulma, 21. yüzyılın en uzun süren tam Güneş tutulması olacak. Ay'ın gölgesi yeryüzüne Hindistan'ın batısında düşecek. Gölge, Şanghay'da Pasifik Okyanusu'na ulaştığında tutulma süresi 5 dakika 51 saniyeyi bulacak. Tam tutulma süresi Japonya'nın güneydoğusunda, Pasifik Okyanusu'ndaki tam tutulma merkezinde 6 dakika 39 saniye sürecek. Tutulmayla ilgili ayrıntılı bilgi için: http://eclipse.gsfc.nasa.gov.

Satürn'ü akşam gökyüzünde görmek isteyenler için bu yılın son fırsatları. Gezegen, ayın başlarında güneybatı ufku üzerinde hâlâ iyi konumda olsa da, ay sonunda alacakaranlığın bitimiyle batıyor olacak. Parlaklığı da giderek azaldığı için Satürn'ün alacakaranlıkta seçilmesi giderek zorlaşacak.

Satürn battığında **Jüpiter** doğu-güneydoğu ufku üzerinde yükselmiş oluyor. -2,8 kadirle parlayan gezegen, gece boyunca gökyüzünde. Ne var ki, gezegen gece yarısı güney yönünde en yüksek konumuna ulaştığında bile gökyüzünde fazla yükselmiyor.

Jüpiter, gece yarısından yaklaşık 3 saat sonra gökyüzünde en iyi konumuna ulaştığı sırada, doğu ufkunda **Mars** ve **Venüs** beliriyor. Geçtiğimiz ayın sonlarına doğru birbirlerine çok yakın konuma gelen iki gezegen artık uzaklaşıyorlar. Mars gökyüzünde yükselirken Venüs konumunu koruyor. İkisi de sabah gökyüzünde sonbahar yıldızlarıyla birlikte görülebilir.

7 Temmuz sabahı, Venüs, Mars ve Ülker açık yıldız kümesi, küçük bir eşkenar üçgen oluşturacaklar. 19 Temmuz'da üçgen bozulmuş olsa da, Ay da manzaraya katılacak.



19 Temmuz sabahı doğu ufku

Merkür, ayın ilk birkaç günü zor da olsa sabah gökyüzünde görülebilir. Ufkun üzerinde hızla alçalan gezegen, 13 Temmuz'da akşam gökyüzüne geçecek. Ancak, ayın sonlarında bile ufkun üzerindeki yükselimi fazla artmayacak.

Ay, 7 Temmuz'da dolunay, 15 Temmuz'da sondördün, 22 Temmuz'da yeniay, 29 Temmuz'da ilkdördün hallerinde olacak.

Geceleyin Dünya

gokyuzu@tubitak.gov.tr



2009 Dünya Astronomi Yılı özel projelerinden biri olan "Geceleyin Dünya" (The World At Night - TWAN) kapsamında, yeryüzündeki en güzel yerlerin ve tarihi eserlerin gece gökyüzü eşliğindeki fotoğrafları toplanıp sergileniyor. Projedeki fotoğraflar, gökyüzü ve manzara fotoğraflarıyla dünya çapında tanınmış, 20 gökyüzü fotoğrafçısının eserlerinden oluşuyor. Bu fotoğrafçılar arasında Türkiye'den bir gökyüzü fotoğrafçısı, Tunç Tezel de bulunuyor.

"Objektifinizden Gökyüzü" başlığı altında okuyucularımızın gökyüzü fotoğraflarını yayımladığımız bu sayfayı, Dünya Astronomi Yılı süresince bu muhteşem fotoğraflara ayıracağız. Her sayıda TWAN fotoğrafçılarının eserleri arasından seçtiğimiz fotoğrafları burada yayımlayacağız.

Gökyüzü köşesinde ve öteki sayfalarımızda okuyucularımızın göndereceği fotoğraflara yer vermeyi sürdüreceğiz.
Bu nedenle sizlerden fotoğraflarınızı kısa bir açıklamayla birlikte (çekim yeri, kullanılan donanım, poz süresi, diyafram açıklığı, ISO değeri vs.) göndermeyi sürdürmenizi bekliyoruz.

Fotoğrafların gokyuzu@tubitak.gov.tr adresine elektronik olarak gönderilmesi; JPEG formatında ve en az 1700 piksel genişlikte olması gerekiyor. Gönderilen fotoğraflar bir elemeden sonra dergide yayımlanacak. Fotoğrafların ana teması gökyüzü, gökcisimleri olmalı.
Göndericiler, fotoğraflarının TÜBİTAK yayınlarında fotoğrafçının adının belirtilmesi koşuluyla kullanılabileceğini kabul etmiş sayılır.



Tunç Tezel / TWAN (www.twanight.org)

Uludağ üzerinde Orion Takımyıldızı ve Orionid Göktaşı Yağmuru



Anthony Ayiomamitis / TWAN (www.twanight.org)

Atina'daki Parthenon Tapınağı üzerinden Güneş'in doğuşu

Dokuz Basamaklı Sayı

1'den 9'a kadar olan sayıları dilediğiniz kadar kullanarak dokuz basamaklı bir sayı oluşturacaksınız. Koşulumuz birbirine bitişik olan bütün basamakların birbirini izleyen sayılardan oluşması.

Bu koşullara uyan kaç sayı oluşturulabilir?

Örnekler:
123234567, 898765678, 343434321.

Sayı Toplamları

T10 = 46 + 47 + ... + 54 + 55 = 505
T15 = 106 + 107 + ... + 119 + 120 = 1695
...

T50 = ?

Soru İşareti

Soru işaretinin yerine hangi sayı gelecek?

9876, 26, ?, 5, 3, 2, ...

Kartlar ve Şekerler

A, B ve C olarak adlandıracağımız üç çocuk bir miktar şekeri paylaşmak üzere üç kart hazırlarlar ve bu kartların her birine farklı bir tamsayı yazarlar. Kartları karıştırarak rasgele birer kart seçerler. Çocukların her biri, seçtiği kartta ne yazıyorsa o kadar sayıda şeker alır. Bu kart seçme ve şeker alma turlarını belli bir sayıda tekrar ederler.

Turların sonunda A'nın 21, B'nin 23, C'nin ise 41 şekeri olmuştur.

A, arka arkaya üç turda aynı kartı çekmiştir.

İkinci turda A, B'den daha büyük, B de C'den daha büyük sayılı bir kart çekmiştir.

Son iki turdaki kart dağılımı aynıdır.

Çocukların ilk turda çektikleri kartları bulunuz.

Üçerlik Sayı

1'den kendisine kadar olan sayılar yazıldığında tam olarak üçte biri kadar "3" rakamı kullanılan sayıları "üçerlik sayı" olarak adlandıralım.
Bu tanıma göre 3, 42 ve 45 üçerlik sayılardır.
(Örnek olarak 45 sayısı incelenirse:
1'den 45'e kadar olan sayılar yazıldığında 15 adet 3 rakamı bulunuyor.

Bu sayılar
3, 13, 23, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39 ve 43'tür.

En büyük üçerlik sayıyı bulunuz.

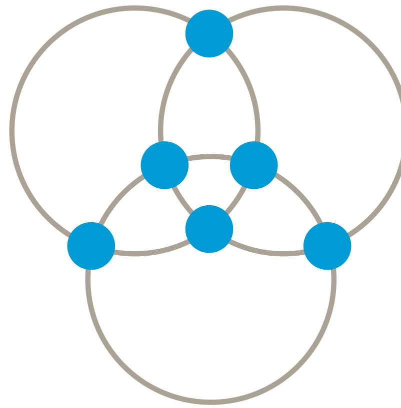
Kurtlar ve Kuzular

Bir bölgede bulunan kurtlar ve kuzularla ilgili aşağıdaki bilgiler bilinmektedir.

- En az iki kurt var.
- Her kurt en az üç kuzuyu parçaladı.
- Herhangi iki kurt (bütün kurt ikilileri) ele alındığında, bu kurtların ikisi tarafından da parçalanan tam tamına bir kuzu var.
- Herhangi iki kuzu (bütün kuzu ikilileri) ele alındığında, bu kuzuların ikisini de parçalayan en az bir kurt var.
- Kurtlardan biri beş kuzu parçaladı.

Kaç kurt, kaç kuzu var?

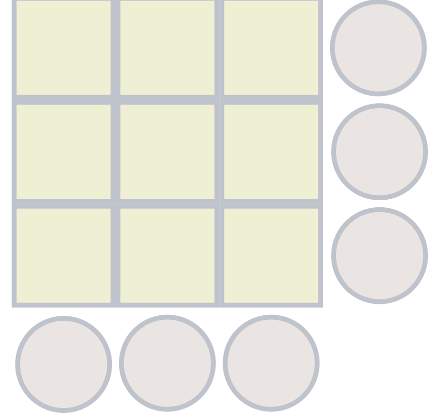
On Altı Daire



Şekilde görüldüğü gibi 3 daire ile en fazla 6 kesişim noktası elde edilebilir. 16 daire ile en fazla kaç kesişim noktası elde edebilirsiniz?

Altı Düğme

3x3'lük bir kareye altı adet düğmeyi öyle yerleştirin ki hiçbir sırada, kolonda ve diyagonalde üç adet düğme yan yana bulunmasın.



Toplamdan Sonuca

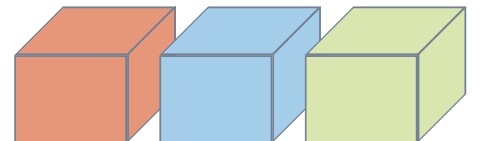
1 ile 1000 gram arasında değişen 1000 adet ağırlığı (1, 2, ..., 999, 1000) kırmızı, mavi ve yeşil renkli üç kutuya öyle yerleştirin ki;

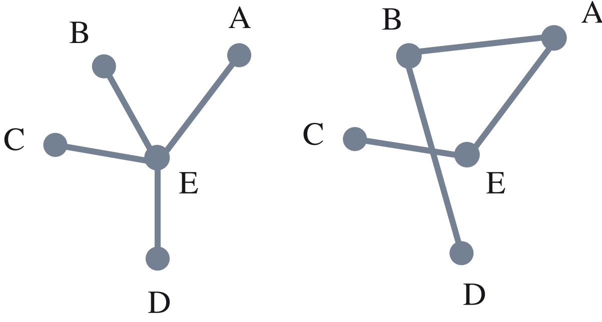
Her kutuda en az bir ağırlık bulunsun.

Kutulardan birinde
sadece tek sayı olan ağırlıklar,
diğerinde
sadece çift sayı olan ağırlıklar
bulunabilir.
Üçüncü kutuda ise iki tür ağırlık da bulunabilr.

Rasgele iki kutu seçilip bu kutulardan rasgele seçilen birer ağırlığın toplamı size verildiğinde diğer (seçilmeyen) kutunun rengi kesinlikle bulunabilsin.

Ağırlıklar bu koşulları sağlayacak biçimde kutulara nasıl yerleştirilmelidir?





Elektrik Anahtarları

Hiçbir üçü aynı doğru üzerinde olmayan beş elektrik anahtarı, dört bakır telin oluşturacağı doğru parçalarıyla birbirine bağlanacaktır. Bu işlem kaç değişik şekilde gerçekleştirilebilir?

Teller plastikle kaplı olduğu için birbirlerinin üzerinden geçebilir.

Bazı bağlantı örnekleri yanda verilmiştir.

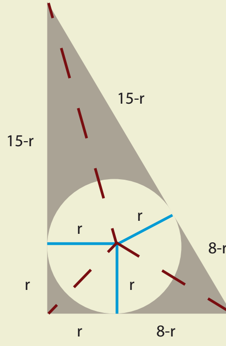
Geçen Sayının Çözümleri

Daire-Dik Üçgen

3 birim

17=(15-r) + (8-r)

‣ r=3



Gazeteciler

8 telefon seansı.
9 gazeteci (A,B,C,...,I) olsaydı,
6 telefon seansı yeterli olacaktı:

	1	2	3	4	5	6
	ABC	DEF	GHI	ADG	BEH	CFI
A	ABC			ABCDEFGHI		
B	ABC				ABCDEFGHI	
C	ABC					ABCDEFGHI
D		DEF		ABCDEFGHI		
E		DEF			ABCDEFGHI	
F		DEF				ABCDEFGHI
G			GHI	ABCDEFGHI		
H			GHI		ABCDEFGHI	
I			GHI			ABCDEFGHI

Bundan sonraki eklenecek her 2 kişi için (veya 1 kişi için) iki konuşma daha eklenirse amaca ulaşılır. Sorumuzda 11 gazeteci verildiği için X ve Y'yi ekleyelim. A'nın bu iki kişiyle yapacağı iki konuşma (biri en başta, diğeri de en sonda olmak üzere) problemi çözer.

1	2	3	4	5	6	7	8
AXY	ABC	DEF	GHI	ADG	BEH	CFI	AXY

Kartların Sırası

En az 10 hamle gerekir. Olası çözümlerden biri:
12345, 21345, 23145, 23415, 23451, 23541, 25341, 52341, 53241, 53421, 54321.

Kumaş Bölmek

42 birim.
Siz 42 birimlik kumaşınızı 15 eşit parçaya ayırırsınız, arkadaşınız ise 7 birimlik kumaşını 3 eşit parçaya ayırır.

Evet Sayısı

160 öğrenci var.
D1 = Doğrucu erkekler
D2 = Doğrucu kızlar
Y1 = Yalancı erkekler
Y2 = Yalancı kızlar

İlk dört soruya verilen EVET sayısı=50+60+70+80=260
Takip eden üç soruya verilen EVET sayısı=25+30+35=90
Son üç soruya verilen EVET sayısı=30+40+50=120

D1+D2+3Y1+3Y2=260
D1+2Y1=90
D2+2Y2=120
denklemleri kullanılarak,
D1+D2+Y1+Y2 = 160 bulunur.

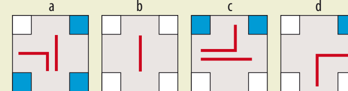
Sayı Grupları

6, 9, 10, 12, 32.

Saat-Dakika-Saniye

a) 22 kez b) 1438 kez c) 1416 kez d) 2 kez

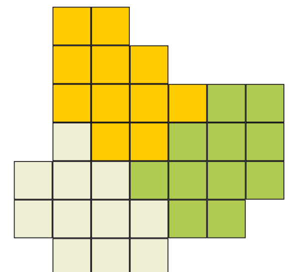
Soru İşareti



a. Doğru parçası sayısı kadar mavi kare var.

Üç Parça

Sağ taraftaki çizimde bölünme gösterilmektedir.



Adem Uludağ

Big Bang'in Romanı

Büyük Patlama ve Evrenin Başlangıcı

Çev. Kemal Küçükgedik
Özgür Yayınları, 2009

"İnsanlar binlerce nesildir gökyüzüne bakmaktalar, ancak bizler evrenin yaratılışı hakkında saygın, mantıklı ve aklı başında bir açıklamaya sahip ilk nesil olmanın ayrıcalığını yaşıyoruz" diyor Simon Singh, modern kozmolojinin tarihini incelediği *Big Bang'in Romanı*'nın başında. Singh'in kuşağımızla ilgili "ayrıcalıklı" nitelemesi bir bakıma az bile. Modern insanın aşağı yukarı 30.000 yıllık bir geçmişi var. Yazılı tarih aşağı yukarı 5000 yıl öncesine uzanıyor. Akıl almaz derecede sıcak ve yoğun bir başlangıçla ortaya çıkmış, genişleyen bir evrende yaşıyor olduğumuz sonucunaysa topu topu 45 yıl öncesinde ulaştık.

Simon Singh'in *Big Bang'in Romanı*'nda anlattığından daha büyük ve etkileyici bir hikâyeyi zihinde canlandırmak belki mümkün olsa bile herhalde kolay değildir. Giderek boyutlanan bu kozmolojik hikâyeyi Singh, gayet hızlı bir biçimde, renkli anekdotlarla ve kayıtlı tarihin sunduğu çerçeveyi yeniden ve gayet anlaşılır şekilde kurarak aktarıyor. Yerkürenin büyüklüğünü ilk ölçme girişimleri ve yıldızlarla ilgili gözlemlerden kuasarlar ve karanlık maddenin keşfine, Eski Yunan filozoflarından Copernicus'a, sonra Einstein ve yirminci yüzyılın geri kalanına, seri adımlarla ama yormadan ilerliyor Singh. Okuru uzay ve zamanda, Ptolemaios sisteminin çıkışsız sınırlarıyla bugün artık 10 milyar ila 20 milyar yıllık bir geçmişi olduğunu bildiğimiz genişleyen evrende ve milyarlarca ışık yılıyla ölçülen mesafelerde gezdiriyor.

Kod Kitabı: Eski Mısır'dan Kuantum Kriptolojisine Gizlilik Bilimi ve çok satan *Fermat'nın Son Teoremi*'nin yazarı olan Singh, *Big Bang'in Romanı*'nı gayet anlaşılır ve eğlenceli bir ders kitabı gibi düzenlemiş. Gerekli bölümlerde anahtar bilimsel kavramlar ile bu kavramları ortaya koyanları, açıklama şemalarında, Büyük Patlama kuramıyla sonuçlanan evrimsel çizgideki konumlarıyla ele alıyor. Bilimsel düşünceleri açıklamak için mümkün olan her yerde çizim ve grafiklerden yararlanıyor ve anlamakta zorlanılabilecek yerlerde, iyi bir öğreticinin yapması gerektiği gibi tekrarlara başvuruyor. Ancak kitabın aslında bulunan sözlük ve bibliyografya Türkçe basıma konulmamış. Singh anlaşılması zor bilimsel düşünceleri gayet sade bir dille ve bir sohbet havasında anlatmakta olduğu kadar konuya duyduğu büyük ilgiyi okura yansıtmakta da başarılı.

Singh, evrenin yapısı ve tarihiyle ilgili günümüzde ulaşılan bilgileri detaylıca anlatmak yerine kozmolojide bugüne nasıl gelindiğini göstermeyi amaçlıyor. Bunu yaparken, rakip kuramları masaya yatırıp argümanları karşılaştırarak aydınlatıcı bilgiler veriyor. Ayrıca ilginç tarihsel anekdotlarla anlatısını zenginleştiriyor.

Kozmoloji tarihinde üç kez, her birinin akla yatkın göründüğü ya da güçlü taraftarlarının olduğu rakip iki kuramın üstünlük mücadelesine tanık olunuyor. Birbirleriyle çarpışan bu üç kuram çiftinden ilki Güneş sistemimizin yapısıyla ilgili olarak Güneş-merkezli ve Dünya-merkezli tezleri kapsıyor. Bu çarpışma en erken dönemlerden MS 1700'e kadar sürüyor. İkinci kuram çifti, bulutsuların gökadamızın içinde mi yoksa dışında mı olduğu sorusunun cevabında zıtlaşıyor. Bu tartış-

Yazar Hakkında

İngiltere'nin en ünlü popüler bilim yazarlarından Simon Singh'in ailesi 1950'de Pakistan'ın Pencap Eyaleti'nden İngiltere'ye göç etti. Çocukluk yılları Somerset'te geçen Singh, Imperial College London'da fizik öğrenimi gördü. Cambridge Üniversitesi ve CERN'de yaptığı çalışmalarla parçacık fiziği alanında doktora derecesini aldı. 1990'da BBC'nin Bilim Departmanı'na katıldı ve çeşitli programların (örneğin *Tomorrow's World* ve *Horizon*) yapımcılığını ve yönetmenliğini üstlendi. 1996'da, matematik tarihinde en çok öne çıkan problemlerden biriyle ilgili olan *Fermat's Last Teorem* (Fermat'nın Son Teoremi) adlı belgeseli yönetti ve bu eserle BAFTA ödülü kazandı. Belgesel, popüler bilimle ilgili Nova adlı televizyon dizisinin bir parçası olarak ABD'de de yayımlandı. Teoremin Andrew Wiles tarafından ispatlanmasının ardından *The Proof* (İspat) olarak yeniden adlandırılan belgesel Emmy televizyon ödüllerine aday gösterildi. Bu ünlü matematik probleminin hikâyesi Singh'in *Fermat's Last Teorem* (Fermat'nın Son Teoremi) adlı ilk kitabının da konusudur. ABD'de *Fermat's Enigma* adıyla yayımlanan kitap, İngiltere'de matematikle ilgili olup en çok satanlar listesinde ilk sıraya yerleşen ilk kitap oldu.

1997'de ikinci kitabı *The Code Book* (*Kod Kitabı*) üzerine çalışmaya başlayan Singh, şifreler ve kripto analizin tarihini ve tarih üzerindeki etkilerini konu aldığı çalışmasında, içinde bulunduğumuz bilgi çağında kriptolojinin öneminin gittikçe arttığını vurgular. *Kod Kitabı*'nın içeriği de bir televizyon yapımına konu olur. *The Science of Secrecy* (Gizlilik Bilimi) adıyla dört bölüm halinde hazırlanan belgesel filmde, İskoç Kraliçesi Mary'nin yazgısını belirleyen şifrenin hikâyesi, I. Dünya Savaşı'nın seyrini değiştiren Zimmerman Telgrafı, 19. yüzyılda Mısır hiyerogliflerini çözmeye çalışan iki büyük deha arasındaki yarış ve modern şifreleme tekniklerinin internette bilgi güvenliğini nasıl sağladığı anlatılır.

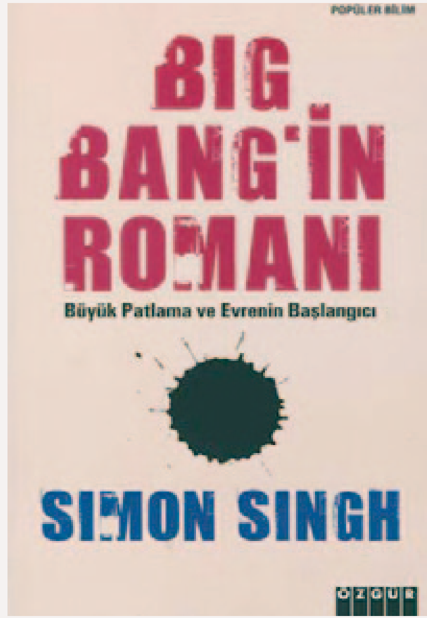


Singh'e 2003'te, eğitim ve bilim iletişimi alanında bilim, teknoloji ve mühendisliğe yaptığı katkılardan dolayı İngiliz Şövalyelik Nişanı verildi. Aynı yıl Loughborough Üniversitesi tarafından onur doktorası (*Honoris causa*), 2005'te ise Southampton Üniversitesi'nce matematik alanında fahri doktora unvanı verildi. 2006'da West of England Üniversitesi'nce, "Bilimin toplumsal algılanışına yaptığı katkılar ve özellikle ortaöğretim okullarında bilim, mühendislik ve matematiği teşvik etme çabalarından ötürü" tasarım doktorası derecesiyle ödüllendirildi. Bunu 2008'de Institute of Physics tarafından, fizik biliminin toplumsal algılanışına katkılarından dolayı verilen Kelvin Madalyası izledi.

Singh'in Edzard Ernst'le birlikte 2008'de yayımladığı *Trick or Treatment?: Aternative Medicine on Trial* ("Tedavi mi Kandırmaca mı?: Alternatif Tıp Yargılanıyor" şeklinde çevrilebilir) son kitabıysa alternatif tıp uygulamalarının bilimselliği üzerine geniş bir inceleme.

ma aşağı yukarı 1800'den 1924'e kadar sürüyor. Kozmik tarihi aydınlatmaya çalışırken, değişme ve hareket halindeki evren modeli ile durağan evren modelini savunan kuramlarsa üçüncü kuram çiftini oluşturuyor. Bu kuramlar arasındaki mücadeleyse 1949'dan 1992'ye kadar sürüyor. Her üç durumda da taraflar güçlü argümanlar ortaya koymuş ve her üçünde de sonunda daha iyi olduğunu ispatlayan kuramın, kanıtlar açısından daha zayıf olduğu dönemler olmuş.

İkinci kuram çiftimizin mücadelesi buna güzel bir örnek oluşturuyor. On dokuzuncu yüzyılın ortalarında gökbilimciler görülebilen bütün yıldızların trilyonlarca kilometre kalınlığı ve bunun on misli büyüklükte eni olan geniş tek bir diske ait olduğunu düşünüyorlardı. Fakat gökyüzünün her yerinde bulanık ışık lekeleri olarak görülen bulutsuların ne olduğu açıklanamıyordu. Bunlar bu diskin, yani gökadamızın içinde mi yoksa dışında mıydı? Her iki taraf da sağlam kanıtlar sunuyordu. Ulusal Bilimler Akademisi 1920'de, bulutsuların diskin "içinde" olduğunu savunanları temsilen Harlow Shapley ile diskin "dışında" olduğunu savunanları temsilen Heber Curtis'in katıldığı büyük bir münazara düzenledi. Shapley tartışmadan "biraz daha iyi olan" taraf olarak çıktı. Ancak üç yıl sonra karşı cepheden Edwin Hubble bulutsuların gökadanın dışında olduklarını kanıtlayan, Sefe değişkeniyle ilgili çalışmasında ulaştığı sonuçları yayımladı. Hubble'ın önden gönderdiği ve sonuçları anlattığı mektubunu okuduğunda Shapley'in verdiği tepki, "İşte evrenimi mahveden mektup" cümlesini sarf etmek oldu. Cevabındaysa "Kendi adıma üzülsem mi yoksa bilim adına sevinsem mi bilemiyorum" diyor ve rakibini tebrik ediyordu.



Singh, *Big Bang'in Romanı*'nda her defasında daha iyi olan kuramın mücadeleyi nasıl kazandığını gösterirken, genel okura bilimsel araştırmanın gelişimi, bilimsel yöntemin doğası ve bilimde çatışmaların nasıl çözüldüğüyle ilgili çok değerli bilgiler veriyor. En büyük bilimsel kuramın tarihi arka planını verirken bilimsel yöntemin değerine ve aklın gücüne ışık tutuyor.

Simon Singh'in Türkçede Yayımlanan Diğer Kitapları

Fermat'nın Son Teoremi

Çev. Sabri Yücesoy
Pan Yayınları, 2001

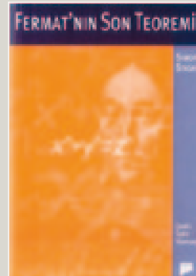
Fermat'nın teoreminin kökleri eski Yunan matematiğindedir. Pierre de Fermat (1601-1665), ortaya Yunanlıların hiç aklına gelmemiş bir soru atar, üstelik çözümün bulunabileceği umudunu uyandıran bir de not bırakır. Kendisinin bu soruya bir yanıtı vardır ama çözümün nasıl olduğunu söylemez. Böylece üç yüz yıl sürecek kovalamaca başlar. Fermat'nın son teoreminin asıl güzelliği, son derece kolayca anlaşılabilecek, basit bir problem oluşudur. Her okul çocuğunun tanıdığı kavramlarla dile getirilebilen bu bulmacayla, Andrew Wiles da okul yıllarında tanışmış ve onu hayatının en önemli tutkusu haline getirmiştir.

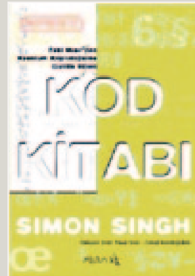
Wiles işe başladığında, sonradan kullanacağı tekniklerden birçoğu henüz bulunmamıştı bile. En iyi matematikçilerin çalışmalarını birleştirmiş, kimsenin cesaret edemeyeceği bir atılganlıkla fikirleri birbirine bağlayıp yeni kavramlar yaratmıştır.

Fermat'nın çözümünde herkes birden çalışmış sayılır, ama birbirinden ayrı ve teoremi ispatlamak gibi bir amaç gütmeden; çünkü bütün modern matematiğin gücünü seferber etmeyi gerektiren bir ispattı bu.

İşte bu kitapta, Fermat öyküsünün tüm zenginliği ve ona hep eşlik etmiş olan tarih ve matematik, kronolojik bir düzen içinde ele alınmış, Pythagoras Kardeşliği'nin devrimci ethos'uyla başlayıp Fermat'nın bulmacasını çözmek için Andrew Wiles'ın verdiği kişisel mücadeleyle sona ermiştir.

Matematikçiler ve matematik sevenler için...





Kod Kitabı

Eski Mısır'dan Kuantum Kriptolojisine Gizlilik Bilimi

Çev. Emin Yaşar Sınır ve
Cemal Hamitoğulları
Klan Yayınları, 2004

İnsanoğlu, yazmaya başladığından beri kodlar kullanarak yazmış ve şifreler, kayıtlı tarih boyunca imparatorlukların kaderini belirlemiştir. Simon Singh, *Kod Kitabı* adlı eserinde şifre çözmenin fırtınalı tarihini anlatmaktadır.

Öykü anlatma yeteneği ile teknik mükemmelliği gerektiren bilimsel yaklaşımı bir araya getirerek şifre çözme yöntemlerinin evrimini ve bu bilimin savaşlar, uluslar ve kişilerin yaşamları üzerindeki dramatik etkilerini ortaya koymaktadır. *Kod Kitabı*, kendi şifreli mektupları yüzünden tuzağa düşürülüp öldürülen İskoç Kraliçesi Mary'den, II. Dünya Savaşı'nın kazanılmasını sağlayan Navaho şifrecilerine, internet sistemlerinin olağanüstü (ve inanılmaz derecede basit) başarısına kadar, tarih boyunca geliştirilmiş en güçlü entelektüel silahın öyküsünü anlatmaktadır: Gizlilik.

Kod Kitabı, baştan sona açık ve kolay anlaşılır teknolojik ve matematik açıklamaları, çoğu korkusuz, bazıları kötü ve tümü de takıntılı olan, dünyadaki en karmaşık kodları yazan ve bunları çözen kişiliklerin portreleriyle tıpkı heyecanlı bir roman tadında. Kolay anlaşılır, etkileyici ve inanılmaz derecede geniş kapsamlı bu kitap, tarihe bakış açınızı değiştirecek, onu yöneten güçleri ve gönderdiğiniz e-postaların gerçekten ne kadar özel olduğunu anlamanızı sağlayacaktır.

TÜBİTAK Bilim ve Teknik Dergisine Gönderilen Yazı ve Görsellerin Sahip Olması Gereken Özellikler

1. TÜBİTAK Bilim ve Teknik dergisi akademik düzeyde yayın yapan bir dergi değildir. Bu nedenle dergimizde yayımlanan yazılar genel okuyucu tarafından anlaşılabilecek düzeyde, net, yalın ve teknik olmayan bir Türkçe ile yazılmış olmalıdır. Yazılar, başlık, sunuş, ana metin, alt başlıklar, çerçeve metinleri ve görsel malzemelerden oluşmaktadır.

Başlık: Konuyu en iyi ifade edebilecek nitelikte, kısa ve ilgi çekici olmalıdır.

Sunuş: Yazının sunuşu başlığın hemen altında yer alır ve konunun önemini, yazının ilginç yanlarını okuyucuda merak uyandıracak biçimde anlatan birkaç kısa cümleden oluşur. Bu kısım sayfa düzeninde farklı bir yazı karakteriyle, ana metinden ayrı biçimde başlığın altında yer alacaktır.

Ana metin: Ele alınan konunun, savunulan düşüncenin ve ilgili olayların örneklerle açıklandığı bölümdür. Yazılar yapılan bir araştırmayı tanıtmaya yönelik olabilir. Ancak bu gibi durumlarda dahi dergimizin bir popüler bilim yayın organı olduğu göz önüne alınarak, yazının önemli bir kısmının konuyu çok genel hatları, temel bilgileri ve kısa bir gelişim tarihçesiyle okura tanıtması gerekmektedir. Burada teknik terimlerin ve temel kavramların net bir şekilde açıklanması beklenmektedir. Yazının geri kalan kısmında araştırmaya özel hususlardan ve araştırmanın genel katkısından bahsedilmeli, önemi ve yaygın etkisi vurgulanmalıdır. Varsa, konu hakkındaki başlıca görüş farklılıklarına işaret edilmeli, ancak ayrıntılı tartışma ve yargılardan kaçınılmalıdır. Çok ender durumlar dışında yazıda formül bulunmamalıdır.

Alt başlıklar: Ana metinde işlenecek konuyla ilgili farklı görüşlerin ve durumların anlatıldığı paragraflar alt başlıklarla ayrılabilir.

Çerçeve metinler: Ana metinde ele alınan konuyu destekleyici, konuya yeni açılımlar getiren, kimi zaman uzmanlar dışındaki okuyucuların anlayamayacağı nitelikteki teknik kavramları açıklayan, kimi zaman uzman görüşlerinin yer aldığı kısa metinlerdir. Çerçeve metinler yazarın kendisi tarafından hazırlanabileceği gibi, konunun uzmanına da yazdırılabilir.

Kaynaklar: Yazının başvuru kaynakları mutlaka liste halinde yazının sonunda verilmelidir. Kaynaklar aşağıdaki örnek biçimlere uygun şekilde yazılmalıdır:

Alp, S., *Hitit Güneşi*, TÜBİTAK Popüler Bilim Kitapları, 2002.

Şeker, A., Tokuç, G., Vitrinel, A., Öktem, S. ve Cömert, S., "Menenjitli Vakalarda Beyin Omurilik Sıvısındaki Enzimatik Değişimler", *Çocuk Dergisi*, Cilt 1, Sayı 3, s. 56-62, 1 Mart 2008.

Soylu, U. ve Göçer, M., "Göller Bölgesi Sulak Alanlar Durum Değerlendirmesi," Göller Bölgesi Çalıştayı, 8–10 Aralık 1995.

http://www.news.wisc.edu/16250

Anahtar kavramlar: Konuyla ilgili en çok beş adet kısa açıklamalı anahtar kavram verilmelidir.

Görsel malzemeler: Yazıda ele alınan düşünceyi destekleyici ve açıklayıcı fotoğraf, çizim, grafik gibi sunuşu zenginleştirici öğelerdir. Görsel malzemeler yayın tekniğine uygun kalitede, yeterli büyüklük ve çözünürlükte (baskı boyutunda en az 300 dpi) olmalıdır. Açıklama gerektiren görsellerin alt ve iç yazıları yazı metninin altında mutlaka verilmelidir. Yazarın önerdiği görsel malzemelerin telif hakkı sorumluluğu yazara aittir. Yazar gerekli izinleri almakla yükümlüdür.

2. Yazı .txt ya da .doc formatında, elektronik ortamda bteknik@tubitak.gov.tr adresine iletilmelidir. Seçilen görsel malzemelerin nerede kullanılması istendiği metinde işaretlenmiş olmalıdır. Görsel malzemeler metnin içinde değil, ayrıca gönderilmelidir.

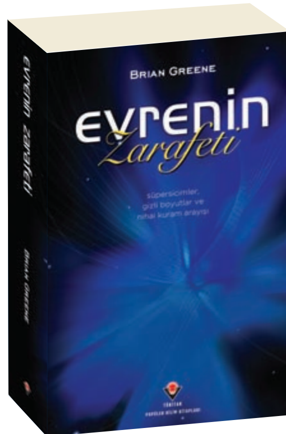
3. Dergi yönetiminden onayı alınmış özel durumlar dışında, bir yazı 2500 kelimeyi geçmemelidir.

4. Yukarıdaki koşulları yerine getirdiği takdirde önerilen yazılar, Yayın Kurulu, Konu Editörleri ve Bilimsel Danışmanlar tarafından değerlendirilir. Yayımlanmasına karar verilen yazılar redaksiyon sürecine alınır ve yazarın onayıyla yazı yayımlanma aşamasına getirilir.

5. Bilim ve Teknik dergisine ilk defa yazı gönderecek kişilerin yazılarını eğitim durumlarını ve/veya yazdıkları konudaki yetkinliklerini gösteren bir özgeçmiş ve fotoğralarıyla birlikte göndermeleri gerekmektedir.

YETİŞKİN KİTAPLIĞI

Evrenin Zarafeti

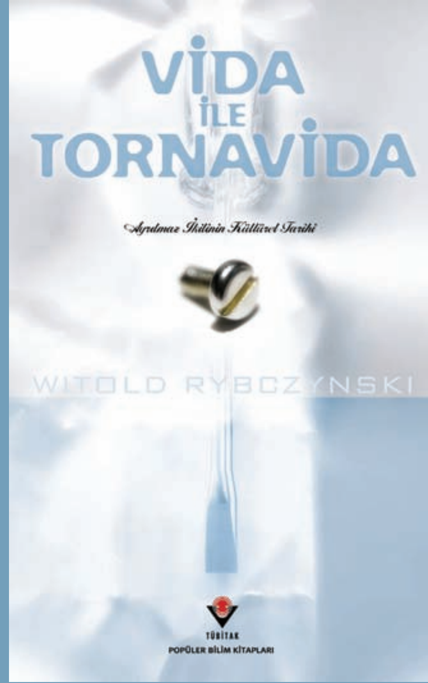


Bir şey keşfetmenin insanın yeni bir şey görmesi değil de bakışını biçimlendirmesi demek olduğu söylenir. Evreni sicim kuramı tarafından biçimlendirilmiş bir bakışla gören okurlar yeni manzaranın nefes kesici olduğunu görecek.

Önde gelen sicim kuramcılarından Brian Greene, çok açık ve anlaşılır bir dille yazdığı bu kitapta okuyucuya nihai kuram arayışının ardındaki bilimsel hikâyeyi ve bilim insanlarının çabalarını anlatıyor. Heyecan verici ve çığır açıcı fikirlerin, örneğin uzayın dokusunda gizli yeni boyutlar, temel parçacıklara dönüşen kara delikler, uzay-zamanda yarıklar ve delikler, birbirlerinin yerine geçebilen çok büyük ve çok küçük evrenler ve bunlar gibi birçok başka fikrin, günümüzde fizikçilerin üstesinden gelmeye çalıştığı bazı sorunların çözümünde çok önemli bir yeri var.

Evrenin Zarafeti bu konuda yapılan keşifleri ve hâlâ çözülememiş gizemleri, durup dinlenmeden uzayın, zamanın ve maddenin nihai doğasını araştıran bilim insanlarının yaşadığı coşkuları ve hayal kırıklıklarını yetkinlik ve incelikle bize aktarıyor. Brian Greene akıllıca kullandığı benzetmelerle, fizikte bugüne kadar ele alınmış kavramlardan en karmaşık olanlarını gerçekten de eğlendirici bir anlatımla okuyucu için kavranabilir hale getiriyor ve bizi evrenin nasıl bir işleyişi olduğunu anlamaya daha önce hiç olmadığı kadar yaklaştırıyor.





Her şey 1999 yılında New York Times'ın editörlerinden David Shipley'nin Witold Rybczynski'den binyılın en iyi ve en kullanışlı aleti hakkında kısa bir makale yazmasını istemesi üzerine başladı.
Rybczynski işi kabul etti ama aletlerin tarihi üzerinde çalışmaya başladığında neredeyse tüm aletlerin kökeninin eskiçağa kadar gittiğini buldu. Oysa o geçtiğimiz binyılın en yararlı ve vazgeçilemez aletini arıyordu.
Tam yazmaktan vazgeçecekken aklına eşinin fikrini almak geldi, eşinin verdiği yanıt ise ilham vericiydi: Tornavidanın ve hemen ardından vidanın aletler sahnesine çıkışı görece yeniydi.
Geç ortaçağ Avrupasının bir icadı olan tornavida Çinlilerin bulmadığı tek önemli aletti.
Bu icadın sahibi Leonardo da Vinci'ydi. Ama yaygın olarak kullanılması uzun zaman almıştı.
Rybczynski akıcı ve eğlendirici üslubuyla kaleme aldığı *Vida ile Tornavida*'da okuyucuya üzerine pek az yazılmış bir konuda yeni bir pencere açıyor.



POPÜLER BİLİM KİTAPLARI